The ONE!

One Schedule to Rule them All!

Welcome to the "One Schedule to Rule them All!". Thank you for your interest by using this. This is an attempt to make things easier for you, the DEF CON attendee, to figure out the when/what/where during the chaos of DEF CON 32.

It started out simple. I had a Kindle and wanted an ebook of the schedule so I didn't have to wear out the paper pamphlet by pulling it out after every talk to figure out where to go next. Back then there was only the main DEF CON tracks, not really any Villages, and production of the ebooks were easy. Over time the Village system developed with a resulting multiplication in complexity, both for attendees and for my production. The offerings no longer include epub and mobi formats and instead now include html, csv, PDF, ical, public Google calendar, and mysql dump format files. Hopefully you'll find something of use.

The intent is still to be a resource to answer the question at the end of an hour of "What's next?"

As a general rule I do not include:

- Off-site events
- Blatent vender pitch events
- Nonspecific timed events. Unfortunately this means the contests aren't on the regular schedule.
- DEF CON events are emphasized, so BSides Las Vegas and BlackHat tend to not show up

Be sure to check out the Links section at the bottom of this. Most all of the events listed here were derived from these links and a Infoboot data feed. There is much more going on at DEF CON than what is listed here.

Check out the Guides/Tips/FAQs links if you're new to Las Vegas.
Notable suggestions are:

- Bring comfortable shoes, you'll be doing a lot more walking than you expect
- Bring a water bottle to keep hydrated
- Beware of going out doors, there's nothing like LV sun and heat
- Everything in Las Vegas is a longer walk than you think
- Relax, don't try to see everything, you'll never be able to!
- Have FUN!

And finally, this is only as good as the ideas and information used to generate it. I welcome your constructive suggestions and comments. Please send them to qumqats@outel.org

Have a good time at DEF CON 32!

Index of DEF CON 32 Activities

Maps List

Maps Browser

Detailed Village Info

Villages Table

Hour by Hour list of happenings, start at the top, or go to a specific day.
Schedule
- Thursday - Friday - Saturday - Sunday

Sorted list of all the Speakers Names linked to their talk's description.
Speaker List

Sorted list of all the Talk's titles linked to the talk description.
Talk Title List
Talk lists for each Village, start at the alphabetic top, or go to a specific Village.
Village Talk List
ADV - AIV - AIxCC - APV - ASV - BBV - BHV - BICV - BTV - CHV - CLV - CON - CPV - DC - DCG - DCGVR - DDV - DL - ESV - HDA - HRV - ICSV - IOTV - LPV - MISC - PHV - PLV - PSV - PYV - QTV - RCV - RFV - RTV - SEV - SOC - TCV - TEV - VMV - WS - XRV

Descriptions and Info for all the talks.
Talk Descriptions

Contests Table
Contests

Demolabs Table
Demolabs

Workshops Table
Workshops

Paid Trainings Table
Paid Trainings

Parties, Gatherings, and Events Table
Parties Gatherings Events

DEF CON 32 Vendors
Vendors

DEF CON 32 Exhibitors
Exhibitors

DEF CON 32 Communities
Communities

The latest news from defcon.org
DEF CON News

The answer to your questsions about DEF CON overall and for this year.
DEF CON FAQ

DEF CON 32 FAQ

DEF CON .org Links

Combined Schedule Sources

Interesting Links

Guides/Tips/FAQs

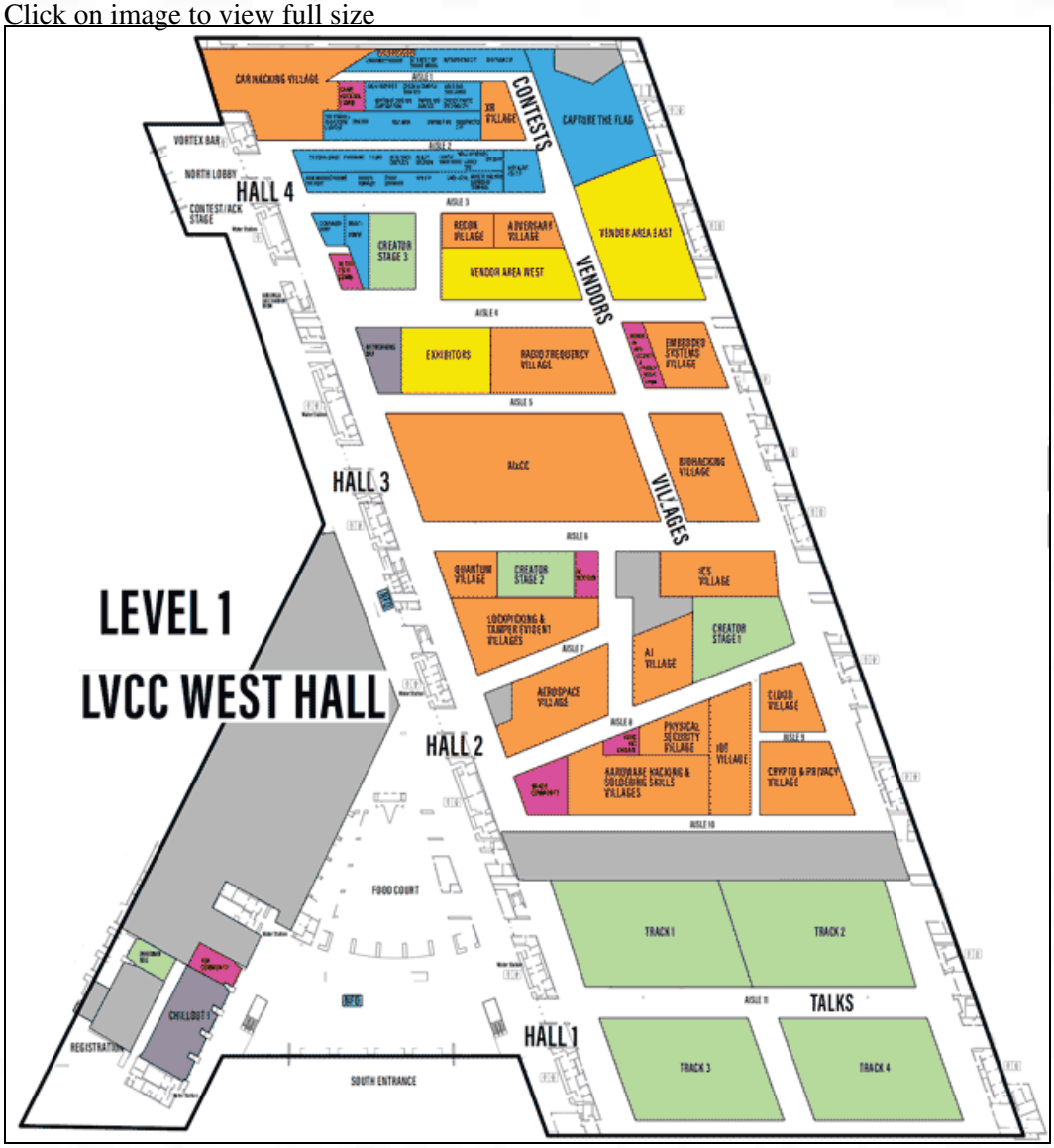
Maps List

Overview of the area around DEF CON 32

Click on image to view full size

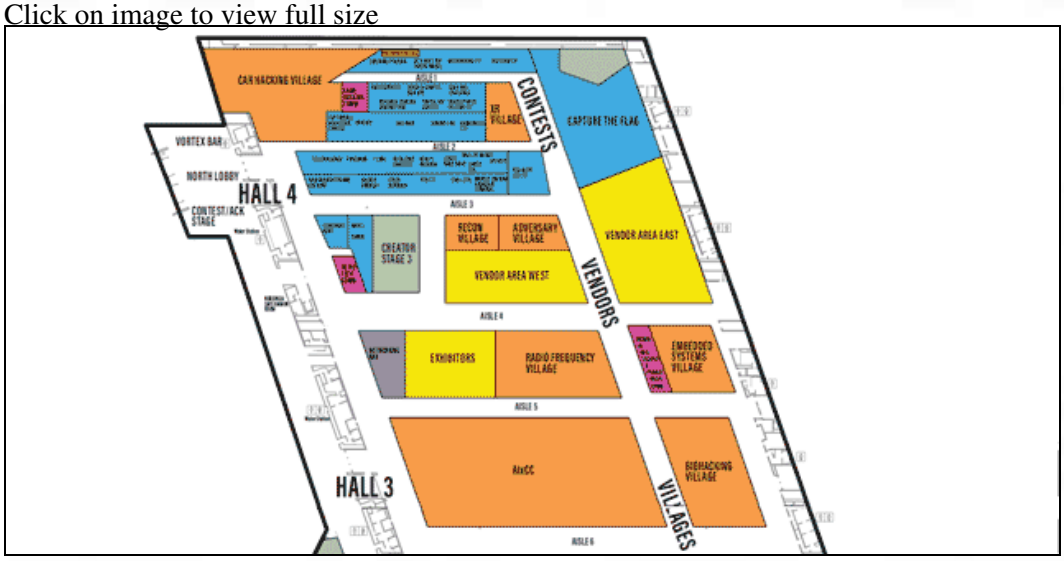
LVCCW Full map of Level 1

Click on image to view full size



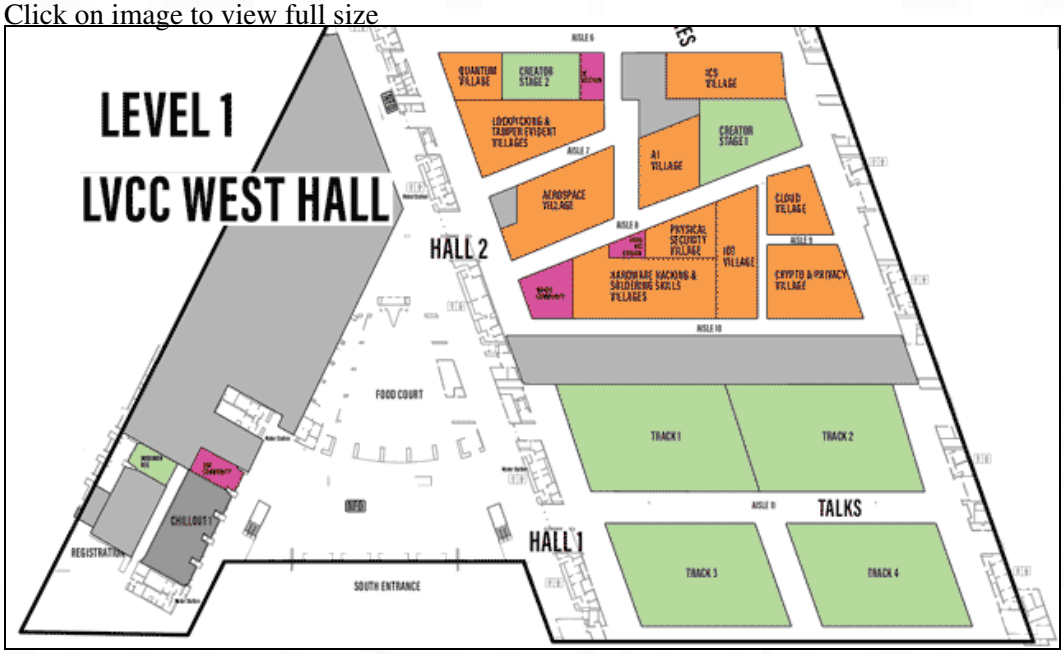
LVCCW map of North portion of Level 1

Click on image to view full size



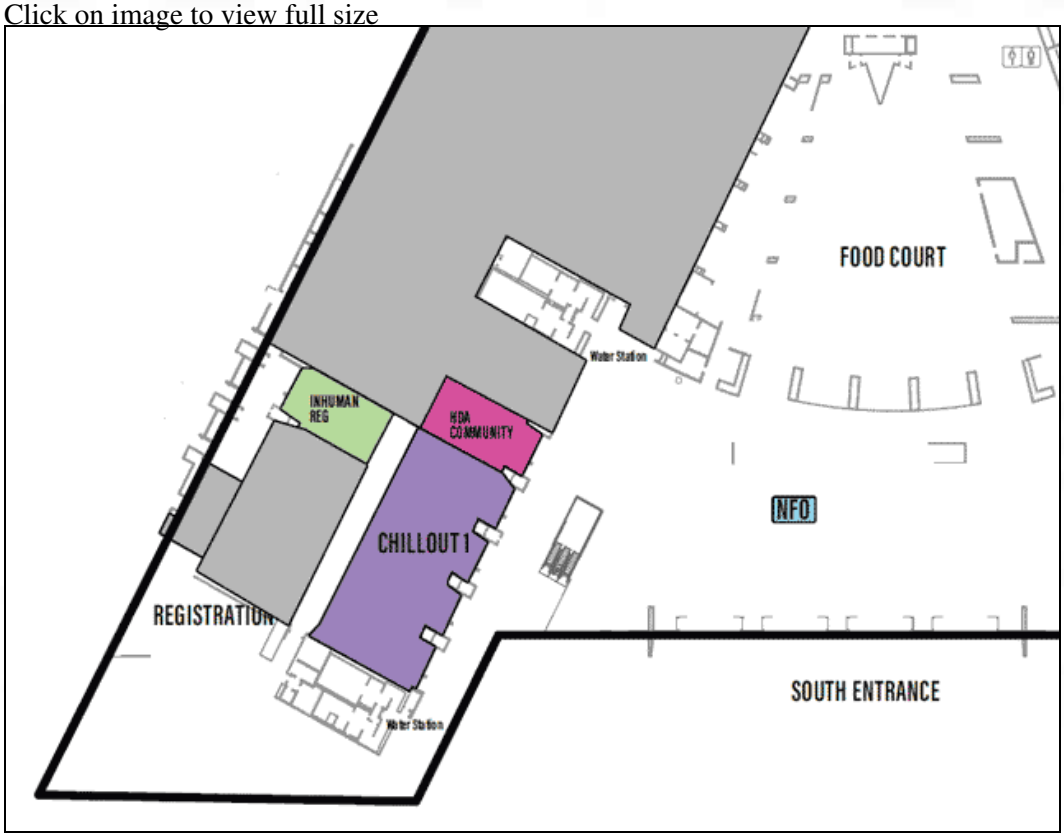
LVCCW map of South portion of Level 1

Click on image to view full size



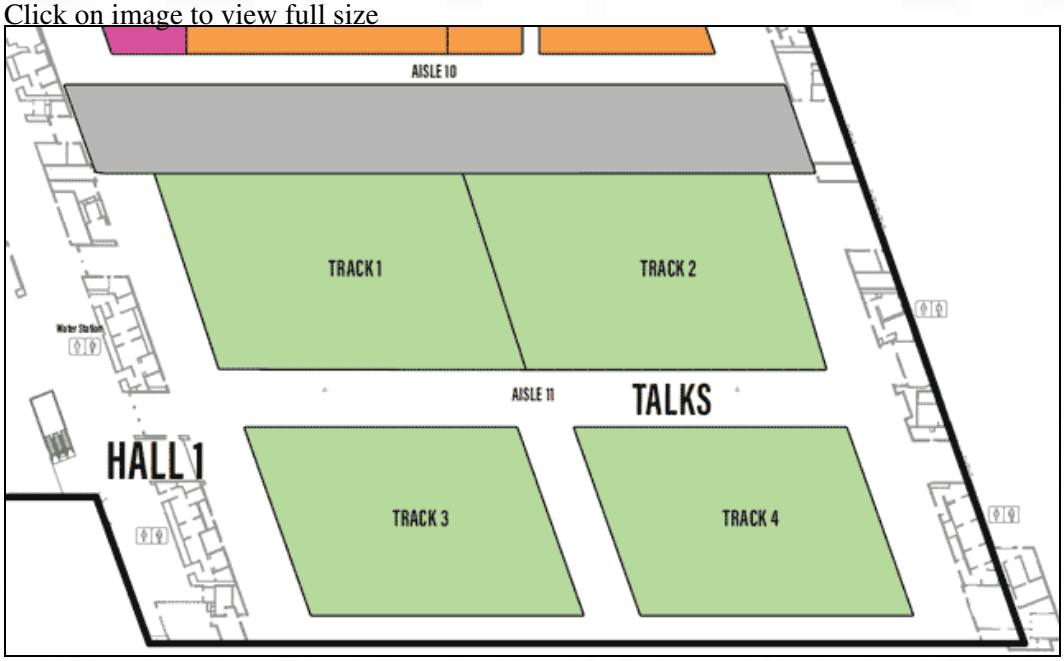
LVCCW map of South Lobby and Registration/HDA of Level 1

Click on image to view full size



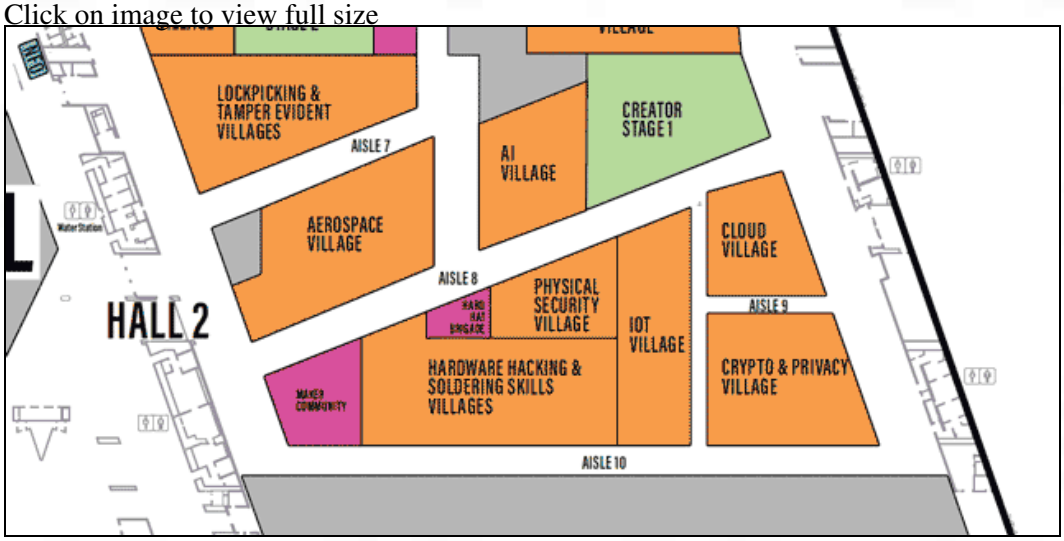
LVCCW map of Hall 1 of Level 1

Click on image to view full size



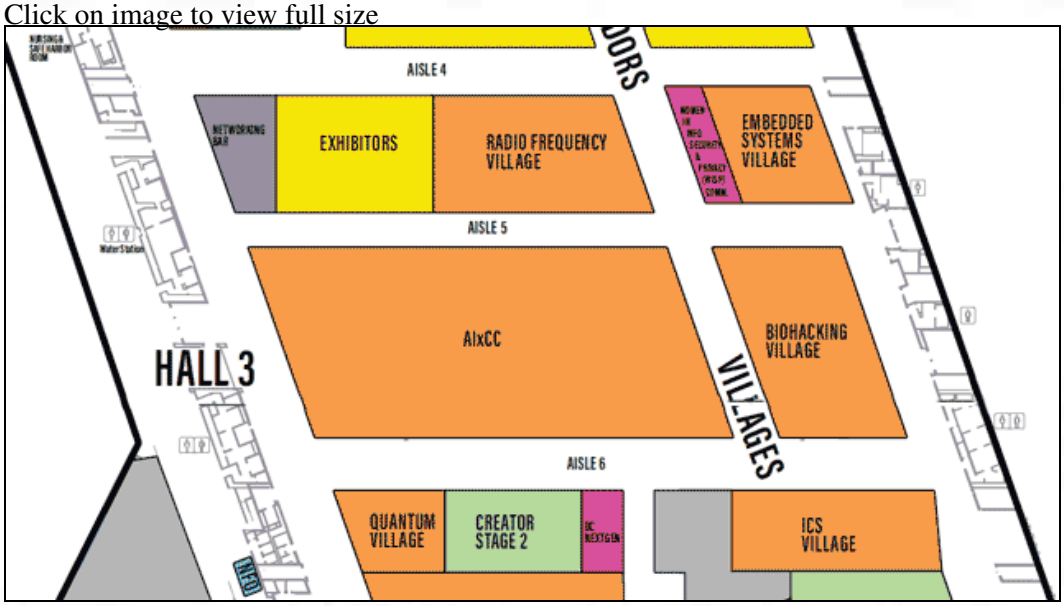
LVCCW map of Hall 2 of Level 1

Click on image to view full size



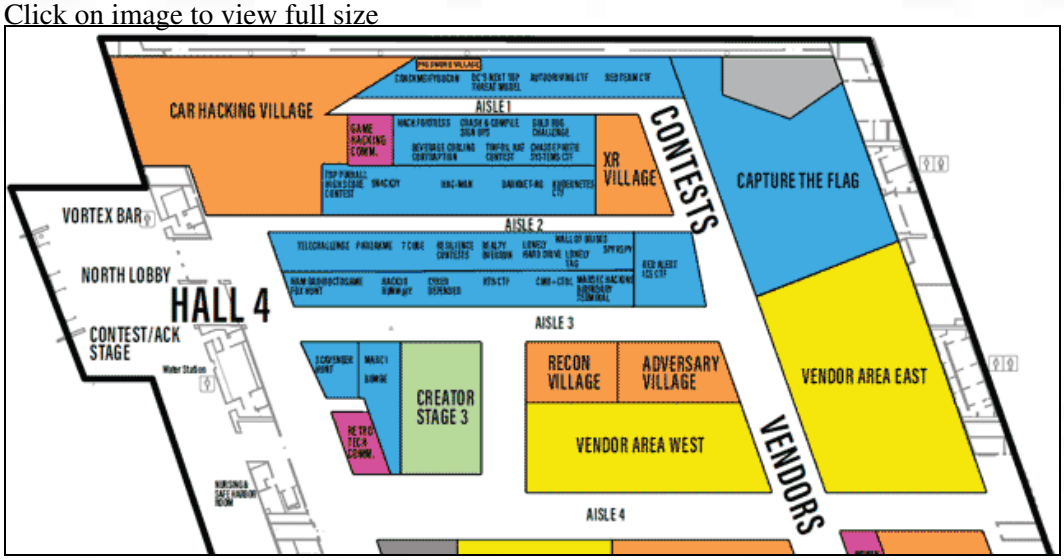
LVCCW map of Hall 3 of Level 1

Click on image to view full size



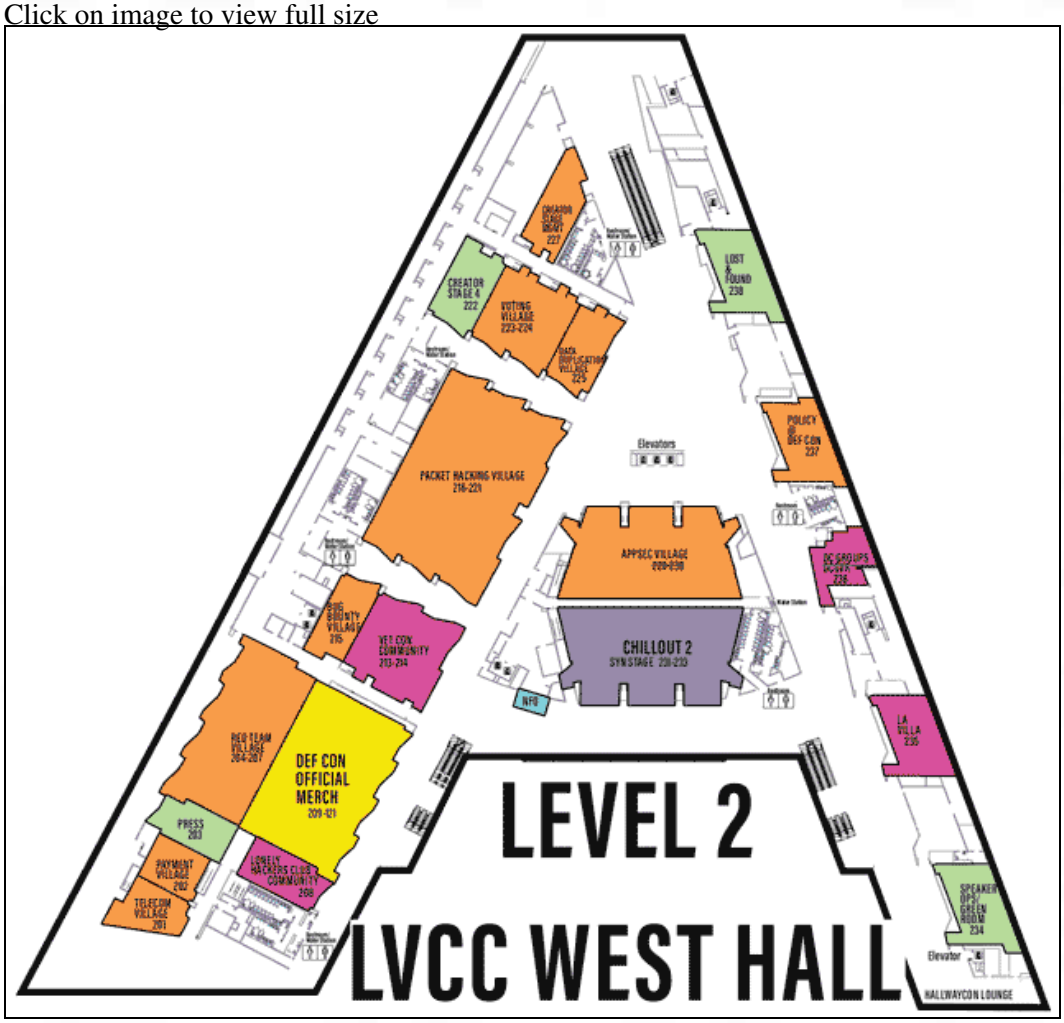
LVCCW map of Hall 4 of Level 1

Click on image to view full size



LVCCW Full map of Level 2

Click on image to view full size

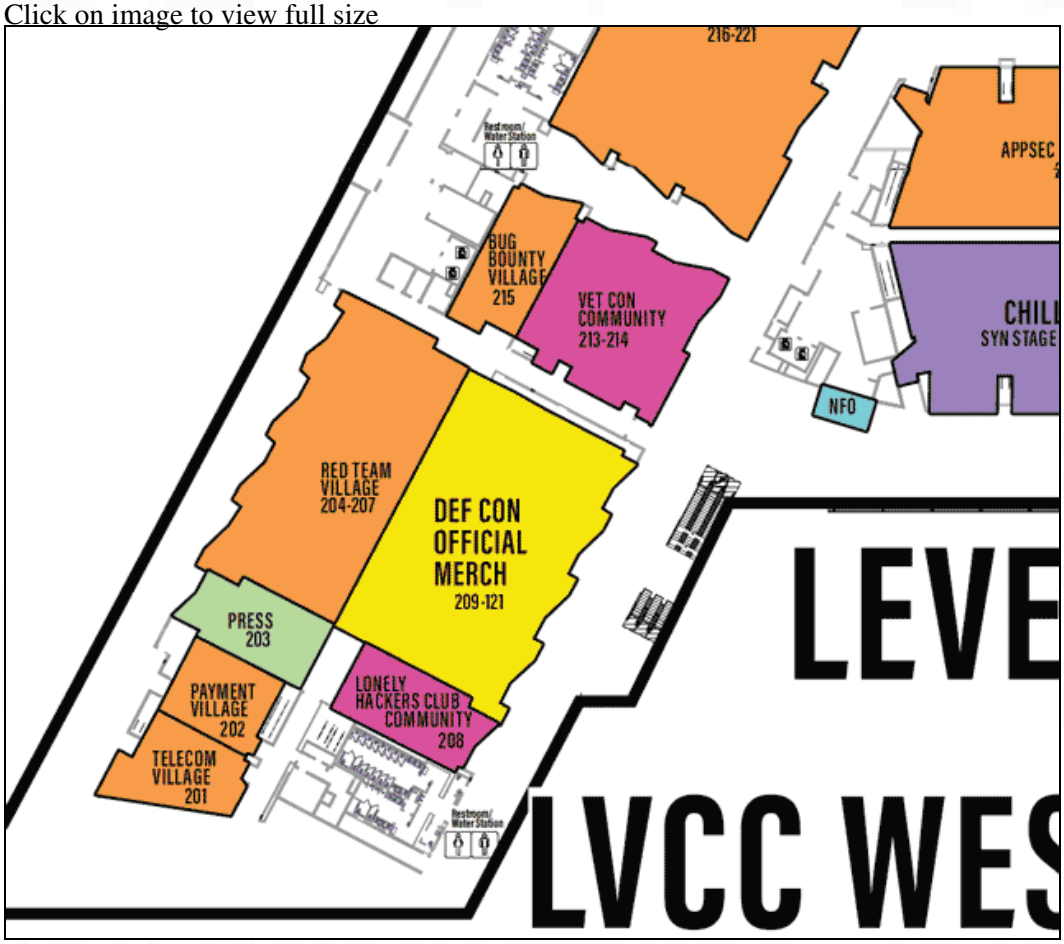


LVCCW map of North portion of Level 2

Click on image to view full size

LVCCW map of West portion of Level 2

Click on image to view full size

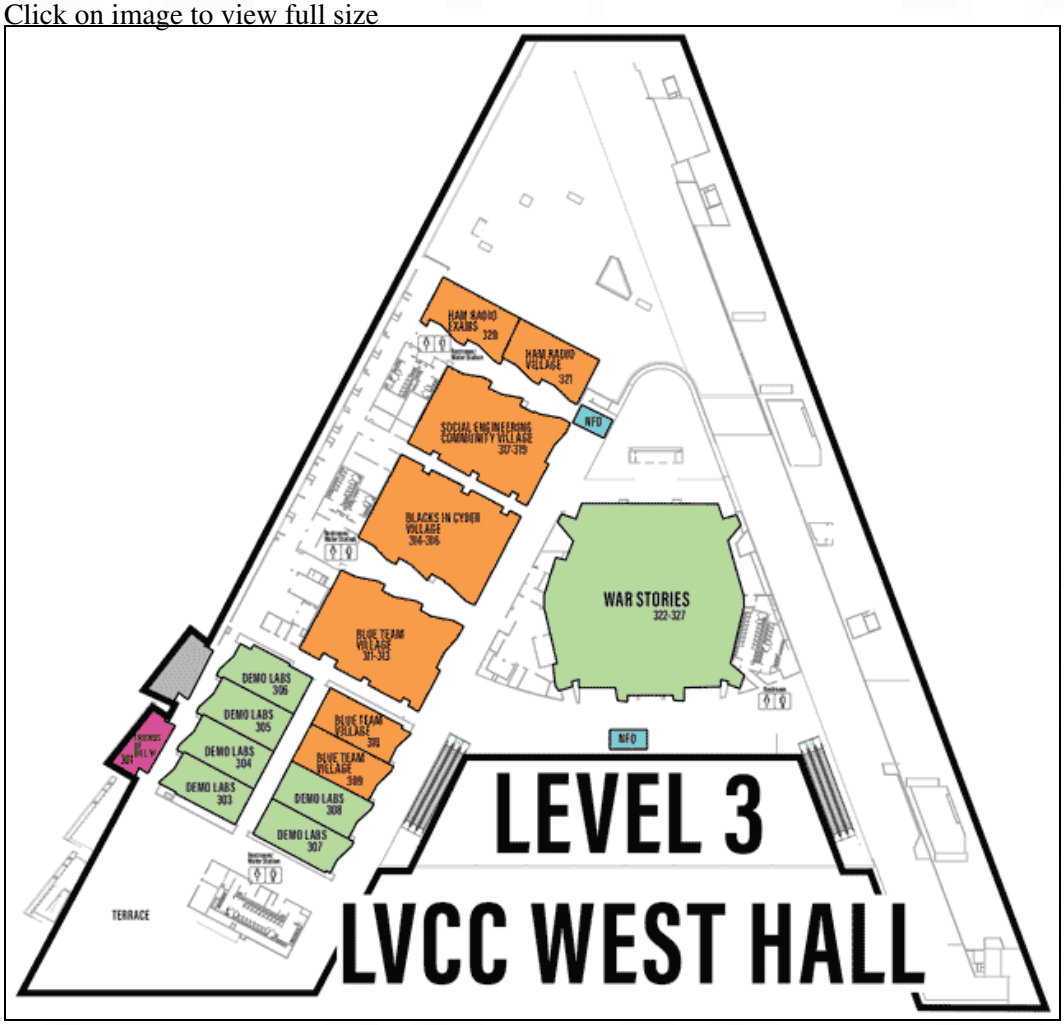


LVCCW map of East portion of Level 2

Click on image to view full size

LVCCW Full map of Level 3

Click on image to view full size

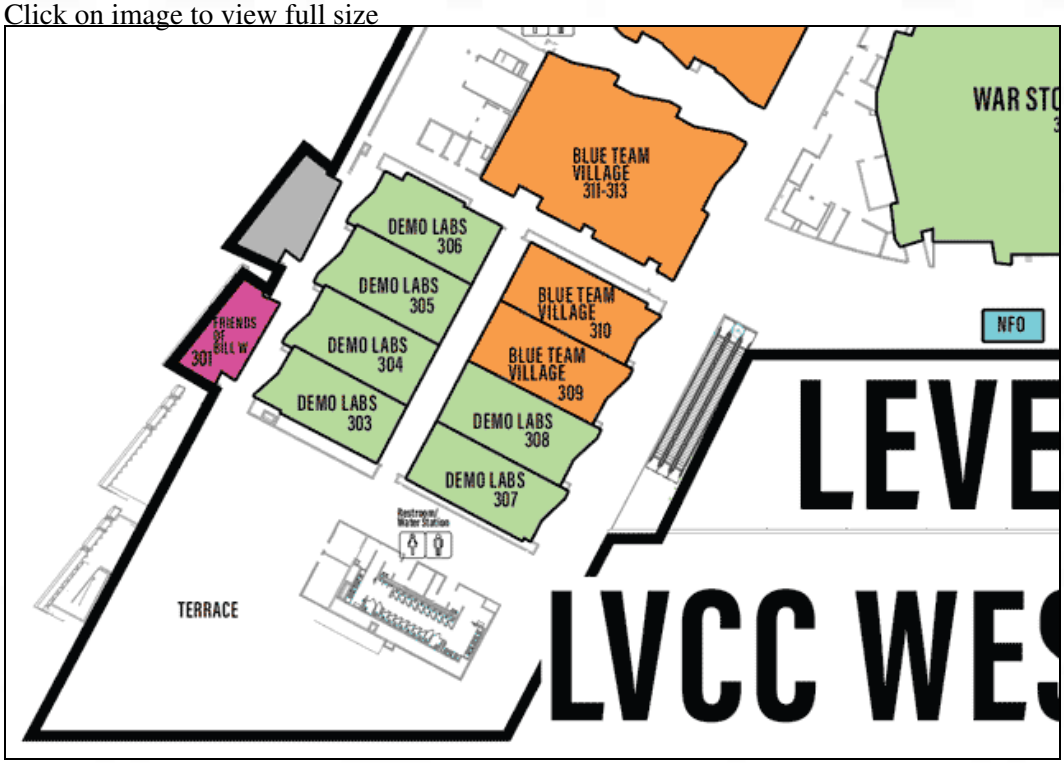


LVCCW map of North portion of Level 3

Click on image to view full size

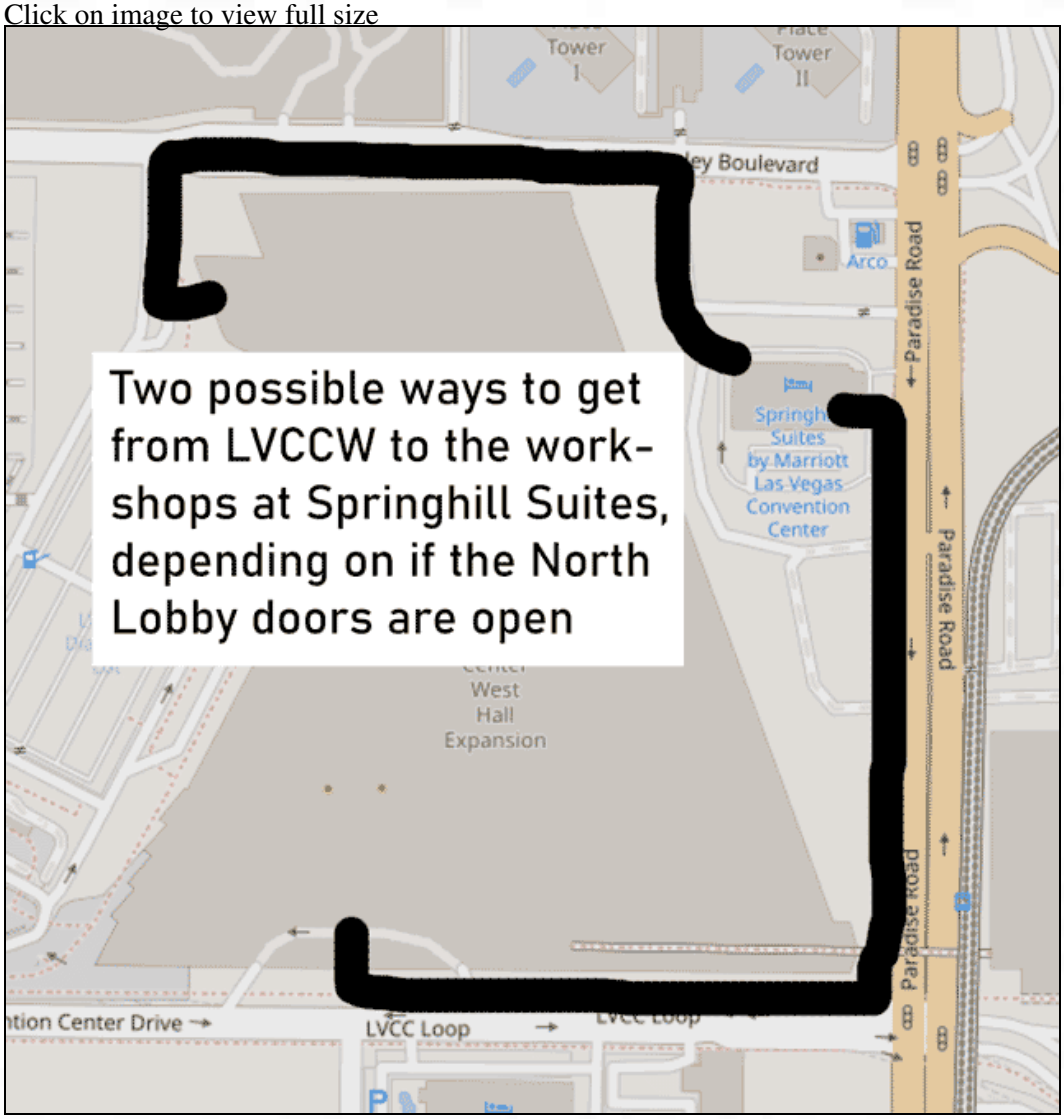
LVCCW map of North portion of Level 3

Click on image to view full size



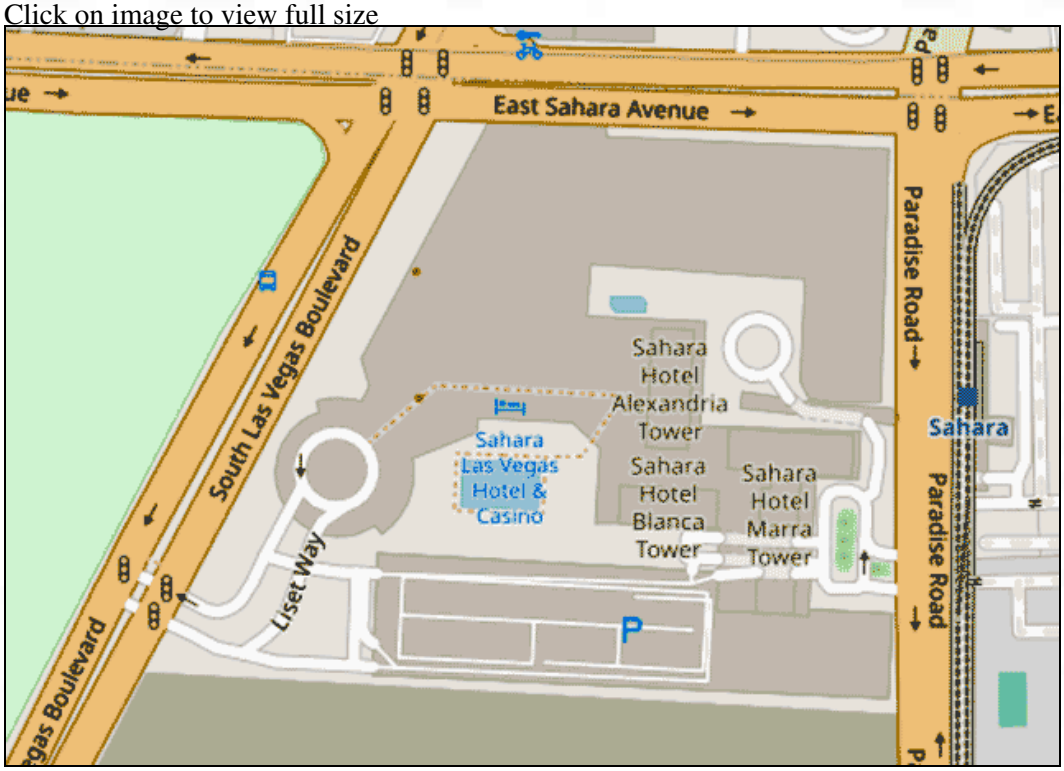
Workshops location - Springhill Suites

Click on image to view full size



Paid Training location - Sahara

Click on image to view full size



Map Browser

LV Strip Overview - Closeup - Sahara - Springhill
L1_Full - L1_North - L1_South
L1_RegHDA - L1_Hall1 - L1_Hall2 - L1_Hall3 - L1_Hall4
L2_Full - L2_North - L2_West - L2_East
L3_Full - L3_North - L3_South
PDF of LVCCW DEF CON 32 map - full rez, best for zooming in
Las Vegas Convention Center - Virtual Tour

Detailed Village Info

ADV - Adversary Village

ADV Village: Talk List
Home Page: https://adversaryvillage.org
Sched Page: https://adversaryvillage.org/adversary-events/DEFCON-32/
DC Village Page: #adversary
DC Forums Page: https://forum.defcon.org/node/248651
Location: LVCC West/Floor 1/Hall 4/HW4-03-05 - Map
Social Media Links:
TW @AdversaryVillag
https://defcon.social/@AdversaryVillage
YT https://youtube.com/AdversaryVillage
DC http://adversaryvillage.org/discord
TI @AdversaryVillage
FB @AdversaryVillage
LI @adversaryvillage

Adversary Village is a community initiative which primarily focuses on adversary simulation, purple teaming, and adversary tradecraft. The village covers adversary emulation, threat/APT/ransomware emulation, breach and adversarial attack simulation, supply chain security, adversary tactics, research on nation-state sponsored threat-actors, adversary intelligence, life, adversarial mindset, adversary philosophy and hacker survival skills.

The goal of the Adversary Village is to build an open security community for the researchers and organizations, who are putting together new means, methodologies towards the simulation and emulation of adversary tactics and purple teaming.

Subsequent to feedback from past editions, Adversary Village shall focus on hosting hands-on deep technical workshops, live demonstrations, panel discussions and a ton of other hands-on activities on adversarial attack simulation/emulation, adversary tactics and hacker survival skills. Adversary Village would have the following hands-on activities for this year at DEF CON;

Adversary simulator and purple teaming hands-on booth: Adversary Simulator booth is a volunteer assisted activity, which has hands-on adversary emulation plans and exercises specific to a wide variety of threat-actors; these are meant to provide the participants with a better understanding of adversarial attack emulation. The booth will be hosting a simulated environment meant to recreate enterprise infrastructure, operational technology environment, which serves targets for various attack simulations.

The hands-on simulator booth also hosts an activity, which would need the participants to generate their own adversary emulation plans to assess the efficacy of the defense systems based on publicly available cyber threat intelligence.

Choose-your-own adversary adventure game: Adversary adventure is a story-scenario based, interactive, choose-your-own adventure model interactive game. This is a gamified version of table-top exercises which is presented to the participants as they can choose to play as an attacker, post exploitation OR a Defender who is defending against an attacker group-threat actor OR even play as a CISO who is dealing with an adversarial situation such as a ransomware incident.

Hands-on deep technical workshops:
Adversary Village will feature a limited number of deep technical workshops focused on advanced adversary tradecraft and techniques.

Adversary Wars CTF:
Adversary Village will be hosting a CTF named "Adversary Wars", where the participants will have to pose as adversaries and replicate adversarial actions against each element of a “target” organization. Adversary Wars would have real world simulation of CTF scenarios and challenges, where the participants can perform various attacks and learn new attack vectors, TTPs, techniques, etc. To visualize the CTF environment, the contest area will feature a miniature model of the city made using interlocking-plastic-bricks. The breached components OR organization buildings will be physically marked in the city model as the CTF progresses.

Just like in previous years, winning teams in the CTF competition can expect fantastic prizes. Additionally, there will be complimentary hoodies (yes, the iconic adversary village hoodies), free t-shirts, cool stickers, village coins, badges, and various other swag for the village participants.

Links:
Mastodon (defcon.social) - https://defcon.social/@AdversaryVillage
Website - https://adversaryvillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248652
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248651
Twitter (@AdversaryVillag) - https://twitter.com/AdversaryVillag

---

Return to Index

AIV - Artificial Intelligence Village

AIV Village: Talk List
Home Page: https://aivillage.org/
Sched Page: https://aivillage.org/events/
DC Village Page: #ai
DC Forums Page: https://forum.defcon.org/node/248648
DC Discord Chan: https://discord.com/channels/708208267699945503/732733090568339536
Location: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map
Social Media Links:
TW @aivillage_dc
TI @aivillage
YT link
DC https://discord.com/invite/GX5fhfT

AI Village is focused on teaching you what you need to know to both defend and break AI. Come learn how ChatGPT, StableDiffusion, malware detectors, ML firewalls, and other AI based products work and how to break them. We have a talks track with world class ML security professionals talking about what they've seen and done in the industry. This year we've expanded the demo area into 8 stations with demos designed to get you up to speed with the underlying technology fast and hands on. Finally, we're running workshops in the morning on dedicated hardware and for the afternoon a generative red team event where you can assess open source models and defenses.

Links:

Website - https://aivillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248649
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248648

Return to Index

AIxCC - Artificial Intelligence Cyber Challenge

AIxCC Village: Talk List
Home Page: https://aicyberchallenge.com/
Sched Page: https://aicyberchallenge.com/
DC Village Page: #aixcc
DC Forums Page: https://forum.defcon.org/node/248672
Location: LVCC West/Floor 1/Hall 3/HW3-05-06 - Map
Social Media Links:
TW @DARPA

The Artificial Intelligence Cyber Challenge (AIxCC) is a two-year competition and educational experience asking the best and brightest in AI and cybersecurity to defend the software on which the world relies. AIxCC will ask competitors to design novel AI systems to secure this critical code and will award a cumulative $29.5 million in prizes to teams with the best systems, including $7 million in prizes to small businesses to empower entrepreneurial innovation during the initial phase of AIxCC.

AIxCC will bring together leading AI companies that will work with DARPA to make their cutting-edge technology and expertise available for challenge competitors. These companies will collaborate with DARPA to enable competitors to develop state-of-the-art cybersecurity systems. AIxCC is collaborating closely with the open-source community to guide teams in creating AI systems capable of addressing vital cybersecurity issues, such as the security of critical infrastructure and software supply chains. Most software, and thus most of the code needing protection, is open-source software, often developed by community-driven volunteers. Further, open-source software comprises most of the code running on critical infrastructure in the United States today, including the electricity and telecommunications sectors.

AIxCC competitions will occur at one of the world's top cybersecurity conferences, DEF CON. The semifinal competition will be at DEF CON 2024, and the final competition at DEF CON 2025, where the top prize will be $4 million.

Links:

Website - https://aicyberchallenge.com/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248673
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248672
Twitter (@DARPA) - https://twitter.com/DARPA

Return to Index

APV - AppSec Village

APV Village: Talk List
Home Page: https://www.appsecvillage.com/
Sched Page: https://www.appsecvillage.com/events/dc-2024
DC Village Page: #appsec
DC Forums Page: https://forum.defcon.org/node/248676

DC Discord Chan: https://discord.com/channels/708208267699945503/790973922949726228
Location: LVCC West/Floor 2/W228-W230 - Map
Social Media Links:
TW @AppSec_Village
LI @appsecvillage
YT https://www.youtube.com/c/AppSecVillage
DC https://discord.gg/5XY8qYXd7R

Come immerse yourself in everything the world of application security has to offer. Whether you are a red, blue, or purple teamer, come learn from the best of the best to exploit software vulnerabilities and secure software. Software is everywhere, and Application Security vulnerabilities are lurking around every corner, making the software attack surface attractive for abuse. If you are just an AppSec n00b or launch deserialization attacks for fun and profit, you will find something to tickle your interest at the AppSec Village.

Software runs the world. Everything from IoT, medical devices, the power grid, smart cars, and voting apps - all have software behind them. Such a variety of topics will be reflected in our cadre of guest speakers representing all backgrounds and walks of life.

AppSec Village welcomes all travelers to choose from talks and workshops by expert community members, an all-AppSec-focused CTF, contests that challenge your mind and your skillz, and more. Bring your thirst for knowledge and passion for breaking things, and your visit to AppSec Village will be thrilling!

Links:

Website - https://www.appsecvillage.com/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248677
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248676
Twitter (@AppSec_Village) - https://twitter.com/AppSec_Village

---

Return to Index

ASV - Aerospace Village

ASV Village: Talk List
Home Page: https://aerospacevillage.org/
Sched Page: https://www.aerospacevillage.org/defcon-32-talk-schedule
DC Village Page: #aerospace
DC Forums Page: https://forum.defcon.org/node/248644
DC Discord Chan: https://discord.com/channels/708208267699945503/732393044363444264
Location: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map
Social Media Links:
TW @secureaerospace
LI @aerospace-village
TW @hack_a_sat
DC https://discord.gg/gV4EWuk
YT https://www.youtube.com/c/AerospaceVillage
https://defcon.social/@aerospacevillage

The aviation and space industries, security researchers, and the public share a common goal: safe, reliable, and trustworthy aviation and space operations. For too long, negative perceptions and fractured trust on all sides have held back collaboration between the aviation, space, and security researcher communities that has advanced safety, reliability, and security of other industries. As the traditional domains of aviation safety and cybersecurity increasingly overlap, more effective collaboration between stakeholders ensures we will be safer, sooner, together.

Through the Aerospace Village, the security research community invites industry leaders, researchers and academia interested in aviation and space security, safety, and resilience to attend, understand, collaborate together to achieve our common goals. Empathy and understanding build common ground, while acts and words likely to increase division between these two communities undermine these efforts. The Aerospace Village welcomes those who seek to improve aviation and space security, safety, and resilience through positive, productive collaboration among all ecosystem stakeholders.

Our Goal

The Aerospace Village is a volunteer team of hackers, pilots, and policy advisors who come from the public and private sectors. We believe the flying public deserves safe, reliable, and trustworthy air travel which is highly dependent on secure

aviation and space operations.

Our Mission

- Create, sustain, and grow an inclusive community focused on aerospace cybersecurity;
- Inspire the next generation of aerospace cybersecurity leaders;
- Promote and develop aerospace cybersecurity expertise and knowledge.

The Aerospace Village will do this by:

- Building connections, trust, and understanding among all Village participants.
- Developing aerospace security skills among DEF CON attendees through workshops and hands-on activities.
- Promoting constructive dialog through talks and interaction.

Links:

Website - https://www.aerospacevillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248645
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248644
Twitter (@secureaerospace) - https://twitter.com/secureaerospace

---

Return to Index

BBV - Bug Bounty Village

BBV Village: Talk List
Home Page: https://bugbountydefcon.com/
Sched Page: https://www.bugbountydefcon.com/agenda
DC Village Page: #bbv
DC Forums Page: https://forum.defcon.org/node/248952
Location: LVCC West/Floor 2/W215 - Map
Social Media Links:
TW @BugBountyDEFCON
YT https://www.youtube.com/BountyTalks
TW @arl_rose
TW @infinitelogins
YT https://www.youtube.com/infinitelogins

The global bug bounty community has witnessed exponential growth, with thousands of members actively engaged in the field. This thriving ecosystem now represents a legitimate and sought-after profession for hackers and cybersecurity specialists. It's time to acknowledge and celebrate this evolution by introducing a dedicated Bug Bounty Village at DEFCON, where hunters, learners, and enthusiasts can converge, interact with top-tier hackers, attend insightful talks, and immerse themselves in hands-on activities.

Our Bug Bounty Village promises to be a focal point for DEFCON attendees. It will feature exclusive talks by some of the world's foremost bug bounty hunters, who will unveil their groundbreaking techniques and share real-world vulnerabilities discovered through their exploits. Furthermore, representatives from leading global companies with established bug bounty programs will provide invaluable insights, guidance, and recommendations for both aspiring hunters and organizations keen on launching their bug bounty initiatives.

Inclusive Learning & Community Engagement:

Our village aims to cater to all levels of expertise, from beginners taking their first steps in bug hunting to seasoned professionals looking to enhance their skills. We will conduct a series of workshops that cover a wide spectrum of topics, ranging from fundamental concepts for newcomers to advanced techniques tailored to the most experienced hackers in the field. Participants will have the opportunity to delve into practical exercises and learn to utilize tools like Portswigger Burp Proxy effectively.

Links:

Website - https://bugbountydefcon.com/
Organizer YouTube (bountytalks) - https://www.youtube.com/c/bountytalks
Organizer YouTube (infinitelogins) - https://www.youtube.com/c/infinitelogins
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248953
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248952
Twitter (@BugBountyDEFCON) - https://twitter.com/BugBountyDEFCON
Twitter (@arl_rose) - https://twitter.com/arl_rose
Twitter (@infinitelogins) - https://twitter.com/infinitelogins

---

Return to Index

BHV - Bio Hacking Village

BHV Village: Talk List
Home Page: https://www.villageb.io/
Sched Page: https://www.villageb.io/creatorstage2024
DC Village Page: #biohacking
DC Forums Page: https://forum.defcon.org/node/248654
DC Discord Chan: https://discord.com/channels/708208267699945503/735273390528528415
Location: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map
Social Media Links:
TW @dc_bhv
LI @biohacking-village
YT http://youtube.com/biohackingvillage
TI @biohackingvillage
DC https://discord.gg/Q8ubDb5
IG @biohacking_village
link

Dive into the Future at the Biohacking Village: Welcome to the Intersection of Biology and Technology

Are you ready to explore the next frontier where technology meets biology? The Biohacking Village at DEF CON invites hackers, cybersecurity experts, biologists, and tech enthusiasts to delve into the exhilarating world of biohacking. This is your unique opportunity to be at the forefront of a revolution that's redefining the boundaries of biology, technology, and human potential.

Why the Biohacking Village?

- Uncover the Unknown: Embark on a journey to explore how hacking skills can unlock new potentials in biotechnology. Discover the secrets of DNA hacking, medical device exploitation, and more.
- Challenge Your Skills: Put your hacking abilities to the test in an entirely new domain. From breaking into sophisticated bioinformatics databases to uncovering vulnerabilities in the latest medical devices, challenge yourself like never before.

- A Hub of Innovation: Witness groundbreaking demonstrations and hands-on workshops led by pioneers in biotechnology and cybersecurity. The Biohacking Village is your chance to see the future as it unfolds.
- Collaborate and Create: Join a diverse community of hackers, scientists, healthcare professionals, and ethicists. Collaborate on projects that push the boundaries of what's possible in health, security, and technology.
- Ethical Hacking for the Greater Good: Use your skills to make a real-world impact. Contribute to projects focusing on improving public health, securing medical data, and enhancing the safety of biomedical devices.

What Awaits You?

- Innovative Talks & Panels: Engage with thought leaders discussing everything from CRISPR gene editing to the cybersecurity of implantable devices.
- Hands-on Workshops: Learn new skills in biohacking, from DIY biology to the art of securing complex bio-systems.
- Live Demonstrations: Experience cutting-edge technology in action, including live hacking of medical devices and bioinformatics systems.
- Networking Opportunities: Connect with like-minded individuals and industry leaders who share your passion for technology and innovation.

Join the Vanguard of Biocybersecurity

At the Biohacking Village, we're not just spectators; we're active participants shaping the future. Whether you're a seasoned hacker or just curious about the intersection of biology and technology, there's something for everyone. Be a part of a community that's breaking new ground and redefining the possibilities of technology and biology.

Embrace your curiosity, unleash your potential, and join us at the Biohacking Village – where the future of biohacking and cybersecurity converges.

Links:

Website - https://villageb.io/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248655
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248654

Return to Index

BICV - Blacks in Cybersecurity

BICV Village: Talk List
Home Page: https://www.blacksincyberconf.com/bic-village
Sched Page: https://www.blacksincyberconf.com/bic-village
DC Village Page: #bic
DC Forums Page: https://forum.defcon.org/node/248660
Location: LVCC West/Floor 3/W314-W316 - Map
Social Media Links:
TW @BlackInCyberCo1
https://defcon.social/@blacksincyber
TI @blacksincybersecurity
YT link
LI @blackincyberconference
PT @blacksincybersecurity
FB @blackincyberconf

The Blacks In Cybersecurity (B.I.C.) Village seeks to bring culturally diverse perspectives to the holistic Cybersecurity community; by way of a series of talks and a capture the flag event. In providing these activities, we hope to help highlight Black experiences, innovations in the field, Black culture and educate the community about Black history. The B.I.C. Village attracts and retains the presence of Hackers from the United States, Africa, Caribbean and Europe (so far) that are a part of the African Diaspora. This often underrepresented and misrepresented community harbors the drive, determination and stick-to-itiveness that is congruent to the Hacker Spirit yet, statistically lacks the proper resources to pursue careers or engage their perspectives on security topics and research.

Through the exposure and information provided by B.I.C. Village, we believe that we can normalize the discussion of deficiency or prejudices in Cybersecurity education/development for minority communities. We also believe this effort can be translated to allow for more diverse hobbyists and professionals to engage and contribute.

Links:

Mastodon (defcon.social) - https://defcon.social/@blacksincyber
Mastodon (infosec.exchange) - https://infosec.exchange/@blacksincyber
Website - http://www.blacksincyberconf.com/bic-village
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248661
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248660

Return to Index

BTV - Blue Team Village

BTV Village: Talk List
Home Page: https://blueteamvillage.org/
Sched Page: https://cfc.blueteamvillage.org/dc32/schedule/
DC Village Page: #btv
DC Forums Page: https://forum.defcon.org/node/248657
DC Discord Chan: https://discord.com/channels/708208267699945503/732454317658734613
Social Media Links:
TW @BlueTeamVillage
TI @blueteamvillage

YT https://www.youtube.com/c/blueteamvillage
DC https://discord.gg/blueteamvillage
https://defcon.social/@blueteamvillage

Welcome to the other side of the hacking mirror. Blue Team Village (BTV) is both a place and a community built for and by people who defend computer systems, networks, and people against cyber attacks. It's a place to gather, talk, share, and learn from each other about the latest tools, technologies, and tactics that our community can use to detect attackers and prevent them from achieving their goals.

Project Obsidian – BTV's Home-Grown Content

The Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Malware Analysis, Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH). Deep dive into technical topics through workshops and exercises that provide practical hands-on experience across each discipline. Project Obsidian workshops provide cybersecurity training that will enable attendees to develop skills needed to be successful in their current and/or future role.

Two of the most valuable takeaways are how to strategically approach a task and the operational processes that support the objectives behind each task. Knowing 'how' to do something is only part of the challenge. Knowing 'when' and 'why' to perform certain tasks adds necessary context to develop the full story of defensive cybersecurity.

Links:

Mastodon (@blueteamvillage@defcon.social) - https://defcon.social/@blueteamvillage
Website - https://blueteamvillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248658
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248657
Twitter (@BlueTeamVillage) - https://twitter.com/BlueTeamVillage

---

Return to Index

CHV - Car Hacking Village

CHV Village: Talk List
Home Page: https://www.carhackingvillage.com/
Sched Page: https://www.carhackingvillage.com/defcon-32-talks
DC Village Page: #ch
DC Forums Page: https://forum.defcon.org/node/248679
DC Discord Chan: https://discord.com/channels/708208267699945503/732722838942777474
Location: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map
Social Media Links:
TW @CarHackVillage
YT http://youtube.com/@carhackingvillage
LI @car-hacking-village
DC https://discord.gg/JWCcTAM

For 10 years, we've been rocking the automotive security scene, and this time, we're cranking up the excitement. Dive into hands-on challenges, snag cool badges, and tackle exercises that'll take your learning to a whole new level! Let's make this DEF CON the most unforgettable yet!

Links:

Website - https://www.carhackingvillage.com
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248680
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248679
Twitter (@CarHackVillage) - https://twitter.com/CarHackVillage

---

Return to Index

CLV - Cloud Village

CLV Village: Talk List
Home Page: https://cloud-village.org/
Sched Page: https://dc32.cloud-village.org/

DC Village Page: #cloud
DC Forums Page: https://forum.defcon.org/node/248682
DC Discord Chan: https://discord.com/channels/708208267699945503/732733373172285520
Location: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map
Social Media Links:
TW @cloudvillage_dc
YT https://www.youtube.com/cloudvillage_dc
DC https://discord.gg/EygUDJABee

With the industry's rapid growth in cloud infrastructure, the presence of an open platform to discuss and showcase cloud research becomes a necessity. Cloud village is an open platform for researchers interested in the area of cloud security. We plan to organise talks, tool demos, CTF and workshops around Cloud Security and advancements.

Our CTF will be a jeopardy style 2.5 days contest where participants will have to solve challenges around Cloud infrastructure, security, recon, etc. These challenges will cover different cloud platforms including AWS, GCP, Azure, Alibaba, Digital Ocean, etc. We will also reward our top 3 teams with awards.

Links:

Website - https://dc32.cloud-village.org
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248683
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248682
Twitter (@cloudvillage_dc) - https://twitter.com/cloudvillage_dc

---

Return to Index

CON - Contests

CON Village: Talk List
Home Page: https://defcon.outel.org/dcwp/dc32/activities/contests-list/
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_CON
DC Forums Page: https://forum.defcon.org/node/248121
Social Media Links:

link

Return to Index

CPV - Crypto Privacy Village

CPV Village: Talk List
Home Page: https://cryptovillage.org/
Sched Page: https://cryptovillage.org/
DC Village Page: #cpv
DC Forums Page: https://forum.defcon.org/node/248685
DC Discord Chan: https://discord.com/channels/708208267699945503/732734002011832320
Location: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map
Social Media Links:
TW @cryptovillage
SL https://cryptovillage.slack.com/
YT link
TI @cryptovillage
https://defcon.social/@cryptovillage

CRYPTO + PRIVACY
VILLAGE

Launched in 2014, Crypto & Privacy Village (CPV) is a community-run village centred on privacy and cryptography that aims to educate and inform the general public, students, educators, hackers, security and privacy professionals, and policymakers. We provide a unique hybrid space that features talks; chill space for relaxing with friends, doing CTFs, and cross industry networking; the Gold Bug Challenge and desk for hints and support; privacy-related art installations; and an information desk for questions about privacy and cryptography. Come talk with us about facial recognition technology, privacy enhancing clothing, or crypto backdoor laws!

Links:

Mastodon (@cryptovillage@defcon.social) - https://defcon.social/@cryptovillage
Website - https://cryptovillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248686
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248685

Return to Index

DC - DEF CON Talks

DC Village: Talk List
Home Page: https://defcon.org/html/defcon-32/dc-32-speakers.html
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_DC
Social Media Links:
TW @defcon
FB @defcon
YT https://www.youtube.com/user/DEFCONConference
http://www.reddit.com/r/defcon
IG @wearedefcon
DC https://discord.gg/defcon

Return to Index

DCG - DEF CON Groups

DCG Village: Talk List

Return to Index

DCGVR - DEF CON Groups VR

DCGVR Village: Talk List
Home Page: https://www.dcgvr.org/
Sched Page: https://www.dcgvr.org/
DC Forums Page:
Social Media Links:
TW @DCGVR
TI @defcon_groups
DC https://discord.gg/bsX4QXf3rD
YT link

Return to Index

DDV - Data Duplication Village

DDV Village: Talk List
Home Page: https://dcddv.org/
Sched Page: https://dcddv.org/dc32-schedule
DC Village Page: #ddv
DC Forums Page: https://forum.defcon.org/node/248949
DC Discord Chan: https://discord.com/channels/708208267699945503/732732641694056478
Location: LVCC West/Floor 2/W225 - Map
Social Media Links:
TW @DDV_DC

The Data Duplication Village has all the updated bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for a copy of all the things, we've got what you need to fill up all your storage including a few nice hash tables and all of the DefCon talks. Add to that just about every other security con talk known to hacker-kind! Our village provides a "free-to-you" service of direct access to terabytes of useful data to help build those hacking skills and talk with other storage enthusiasts.

Check the schedule and/or dcddv.org for the most up-to-date information.

How It Works

The DDV provides a core set of drive duplicators and data content options. We accept 8TB and larger drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in your blank SATA3 drives - check them in early - to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO - get those drives in early!

What You Get

We're working on more content right up until the last minute so keep checking on dcddv.org for the latest. This year, we're adding new data to duplicate! Humans will be able to choose from the following data sources for duplication:

- A) Infocon.org Archive - 6TB archive of all the past hacking convention videos that DT could find, built on last years collection and always adding more for your data consuming appetite.
- B) Rainbow tables 1 of 3 - 6TB from freerainbowtables.com, the Lanman, MSQLSHA1, and NTLM hash tables plus freerainbowtables.com tools
- C) Rainbow tables 2 of 3 - 6TB from freerainbowtables.com, the A5/1 GSM, and MD5 tables plus freerainbowtables.com tools
- D) Vx Underground Archive - 8TB archive of the latest papers, samples, and code from Vx Underground
- E) Rainbow tables 3 of 3 - 8TB of New NTLM-9 hash tables and a copy of the Infocon.org mirrors

Links:

Website - https://dcddv.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248950
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248949

Return to Index

DL - DEF CON DemoLabs

DL Village: Talk List
Home Page: https://forum.defcon.org/node/248122
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_DL

Return to Index

ESV - Embedded Systems Village

ESV Village: Talk List
Home Page: https://embeddedvillage.org/
DC Village Page: #esv
DC Forums Page: https://forum.defcon.org/node/248663
Location: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map
Social Media Links:
TW @EmbeddedVillage

Embedded systems exist at the intersection of hardware and software, built to accomplish a specific task. Often these disciplines are dealt with individually, but understanding the custom relationships between hardware and software is key to performing security research on these devices.

Embedded Systems Village advances the security of embedded systems by hosting hands-on hacking workshops, showcasing new security research demos, and organizing exciting hacking contests to educate attendees and manufacturers on the approach hackers use to attack these devices. Attendees will leave the village with an understanding of how to reduce complex, exotic devices to their underlying embedded components and to extract the information required to use the tools and techniques taught at other villages where embedded systems are on display.

Links:
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248664
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248663

Return to Index

HDA - DEF CON Hackers with Disabilities

HDA Village: Talk List
Social Media Links:
TW @HDA_DEFCON

Return to Index

HHV - Hardware Hacking and Solder Skills Villages

HHV Village: Talk List
Home Page: https://dchhv.org/
Sched Page: https://dchhv.org/schedule/schedule.html
DC Village Page: #hhv
DC Forums Page: https://forum.defcon.org/node/248669
DC Discord Chan: https://discord.com/channels/708208267699945503/732728536149786665
Location: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map
Social Media Links:
TW @DC_HHV
https://defcon.social/@DC_HHV

Every day our lives become more connected to consumer hardware. Every day the approved uses of that hardware are reduced, while the real capabilities expand. Come discover hardware hacking tricks and tips regain some of that capacity, and make your own use for things! We have interactive demos to help you learn new skills. We have challenges to compete against fellow attendees. We have some tools to help with your fever dream modifications. Come share what you know and learn something new.

Links:

Website - https://ddhhv.org/
Mastodon (@DC_HHV@defcon.social) - https://defcon.social/@DC_HHV
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248670
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248669

Return to Index

HRV - Ham Radio Village

HRV Village: Talk List
Home Page: https://hamvillage.org/
Sched Page: https://hamvillage.org/dc32/index.html
DC Village Page: #ham
DC Forums Page: https://forum.defcon.org/node/248666
DC Discord Chan: https://discord.com/channels/708208267699945503/732733631667372103
Location: LVCC West/Floor 3/W321 - Map
Social Media Links:
TW @HamRadioVillage
TI @HamRadioVillage
DC https://discord.gg/hrv
https://defcon.social/@HamRadioVillage

Ham radio is the original group of electronic hackers, starting long before computers, circuit chips, or even transistors. Continuing this pioneer spirit, Ham Radio Village is here to support advancement of the hobby with a cybersecurity slant. Everything we do today involves wireless communications of some sort, and a basic knowledge of how radio works is crucial. In the HRV, you can learn hand-on with topics such as how to legally use a radio to send commands to a satellite, communicating around the globe when no other methods exist, and how to send and receive real-time location data without relying on any cellular networks. You can put your skills to the test by trying to find the hidden transmitters in the Ham Radio Fox Hunt contest, as well as transmitting memes over the airwaves to defcon attendees. We provide license testing services for those looking to become licensed or upgrade their license class, as well as guidance on how to hack on the medium to achieve the best results and have the most fun!

Links:

Mastodon (defcon.social) - https://defcon.social/@HamRadioVillage
Website - https://hamvillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248667
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248666

Return to Index

ICSV - Industrial Control Systems Village

ICSV Village: Talk List
Home Page: https://www.icsvillage.com/
Sched Page: https://www.icsvillage.com/defconevents/def-con-32
DC Village Page: #ics
DC Forums Page: https://forum.defcon.org/node/248688
DC Discord Chan: https://discord.com/channels/708208267699945503/735938018514567178
Location: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map
Social Media Links:
TW @ICS_Village
LI @icsvillage
YT link
TI @ics_village

Mission. ICS Village is a non-profit organization with the purpose of providing education and awareness of Industrial Control System security.

- Connecting public, industry, media, policymakers, and others directly with ICS systems and experts.
- Providing educational tools and materials to increase understanding among media, policymakers, and general population.
- Providing access to ICS for security researchers to learn and test.
- Hands on instruction for industry to defend ICS systems.

Exhibits. Interactive simulated ICS environments that provide safe yet realistic examples to preserve safe, secure, and reliable operations. We bring real components such as Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), Remote Telemetry Units (RTU), and actuators, to simulate a realistic environment throughout different industrial sectors. Visitors can connect their laptops to assess these ICS devices with common security scanners, network sniffers to sniff the industrial traffic, and more! We will also have space dedicated to Maritime technology as well as Escape Rooms ran by Idaho National Labs and CISA. In addition to talks, hands-on demos/hacking, and escape rooms we are collaborating with BioHacking Village to demonstrate how Industrial Control Systems are used in Health Care.

Links:

Website - https://www.icsvillage.com/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248689
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248688

Return to Index

IOTV - Internet Of Things Village

IOTV Village: Talk List
Home Page: https://www.iotvillage.org/
Sched Page: https://www.iotvillage.org/defcon.html#Talks
DC Village Page: #iot
DC Forums Page: https://forum.defcon.org/node/248691
DC Discord Chan: https://discord.com/channels/708208267699945503/732734565604655114
Location: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map
Social Media Links:
TW @iotvillage
TW @ISEsecurity
TW @Villageidiotlab
https://defcon.social/@IoTVillage/
TI @iotvillage
YT https://www.youtube.com/c/IoTVillage/videos
DC https://discord.gg/EFKbNFrFaN

[Hack all the things](https://www.youtube.com/watch?v=JZCmqMz1Wvo) at IoT Village!

IoT Village advocates for advancing security in the Internet of Things (IoT) industry through bringing researchers and industry together. IoT Village hosts talks by expert security researchers, interactive hacking labs, live bug hunting in the latest IoT tech, and competitive IoT hacking contests, including our 4 time black badge DEF CON CTF. Over the years, IoT Village has served as a platform to showcase and uncover hundreds of new vulnerabilities, giving attendees from around the globe the opportunity to learn about the most innovative techniques to both hack and secure IoT. IoT Village is organized by security consulting and research firm, [Independent Security Evaluators (ISE)](https://www.ise.io/).

Follow both ISE (@ISEsecurity) and IoT Village (@IoTvillage) on Twitter for updates on talks, contests, and giveaways.

Links:

Mastodon (defcon.social) - https://defcon.social/@IoTVillage/
Website - https://iotvillage.org/defcon.html
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248692
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248691
Twitter (@iotvillage) - https://twitter.com/iotvillage
Twitter (@ISEsecurity) - https://twitter.com/ISEsecurity

Return to Index

LPV - Lock Pick Village

LPV Village: Talk List
Home Page: https://www.toool.us/
Sched Page: https://x.com/toool/status/1821662290296660451
DC Village Page: #lpv
DC Forums Page: https://forum.defcon.org/node/248927
DC Discord Chan: https://discord.com/channels/708208267699945503/732734164780056708
Location: LVCC West/Floor 1/Hall 2/HW2-07-03-A - Map
Social Media Links:
TW @toool
TI @toool_us
YT https://youtube.com/c/TOOOL-US
https://techhub.social/@TOOOL

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

Links:

Website - https://www.toool.us/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248928
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248927
Twitter (@toool) - https://twitter.com/toool

Return to Index

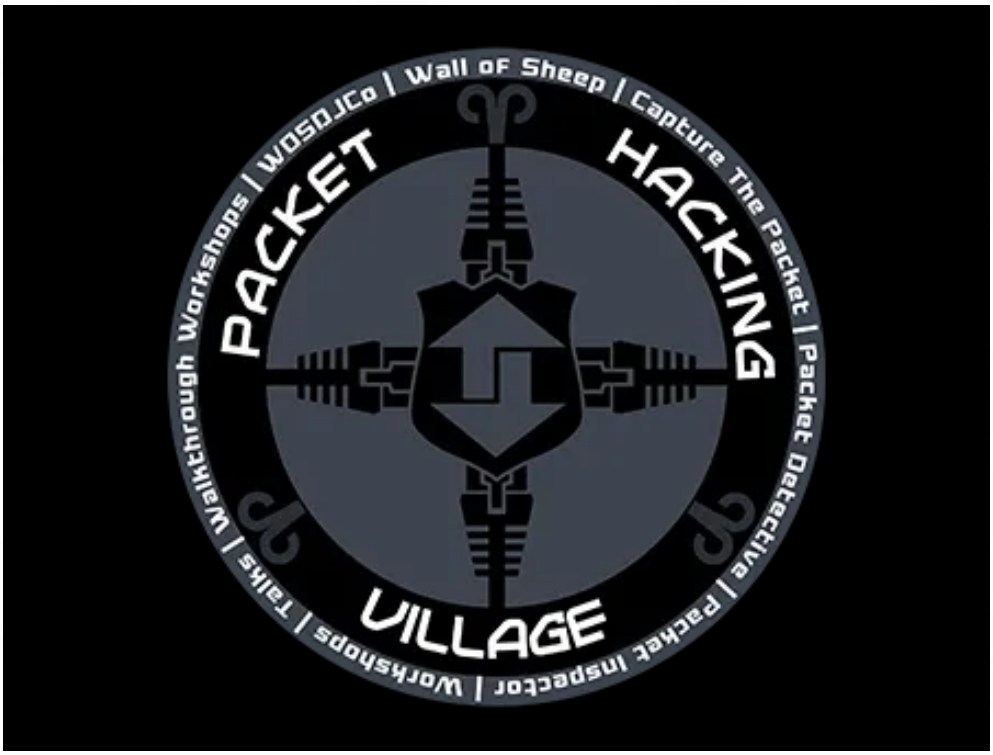
MISC - Misc

MISC Village: Talk List
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_MISC

Return to Index

PHV - Packet Hacking Village

PHV Village: Talk List
Home Page: https://www.wallofsheep.com/
Sched Page: https://www.wallofsheep.com/pages/dc32
DC Village Page: #phv
DC Forums Page: https://forum.defcon.org/node/248889
DC Discord Chan: https://discord.com/channels/708208267699945503/708242376883306526
Location: LVCC West/Floor 2/W216-W221 - Map
Social Media Links:
TW @wallofsheep
FB @wallofsheep
YT https://youtube.com/wallofsheep
TI @wallofsheep
PS https://www.periscope.tv/wallofsheep
https://defcon.social/@wallofsheep
IG @wallofsheep



The Packet Hacking Village at DEF CON provides a community learning experience for people of all skill levels, from absolute beginners to seasoned professionals. While DEF CON is made up of dozens of small community-of-interest villages, we are one of the largest and most well known. We host practical training, network forensics and analysis games, and the renowned Capture The Packet event, which has been a Black Badge contest over 10 times and draws world-class hackers from around the world. Our mission has always been simple: to teach people good internet safety practices, and to provide an atmosphere that encourages everyone to explore and learn.

We provide a welcoming environment for hackers of all skill levels and backgrounds to network, learn new things, and be active participants in DEF CON. Our famous “Wall of Sheep” provides a fun and interactive take on internet security and privacy, while our contests Packet Inspector, Packet Detective, and Capture The Packet serve as a zero-to-hero pathway for individuals to learn network security, packet analysis, and delve into advanced security topics. Every year we strive to bring something new and innovative to DEF CON, whether it’s never-seen-before talks or creative games to teach and test skills.

Depending on what talks, contests, and events participants select, they can expect to learn any/all of the following:

Basic Internet security and privacy, network cable construction, honeypot setup and operation, regex, Linux training, packet interception and decoding, network analysis, sniffing, and forensics, reverse engineering, file forensics, system forensics, cryptography analysis, and more to be determined by the talks and workshops that we accept.

The Packet Hacking Village and Wall of Sheep have been a part of DEF CON since DEF CON 9, and we are proud to provide education and training to the hacker community at no cost.

Links:

Facebook - https://www.facebook.com/wallofsheep
Instagram - https://www.instagram.com/wallofsheep/
YouTube - https://www.youtube.com/channel/UCnL9S5Wv_dNvO381slSA06w
Mastodon (defcon.social) - https://defcon.social/@wallofsheep
Pinterest - https://www.pinterest.com/wallofsheep/
Tumblr - https://wallofsheep.tumblr.com/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248890
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248889
Twitter (@wallofsheep) - https://twitter.com/wallofsheep

Return to Index

PLV - Policy Village

PLV Village: Talk List
Home Page: https://defcon.org/policy/
DC Village Page: #policy
DC Forums Page: https://forum.defcon.org/node/248898
Location: LVCC West/Floor 2/W237 - Map
Social Media Links:
TW @DEFCONPolicy
link
https://defcon.social/@defconpolicy

The DEF CON community understands that creating a safer digital society requires collaboration between security and policy experts. Policy @ DEF CON provides a space for representatives of all areas of security to come together to educate and engage each other.

Tech policy is being written as we speak and we believe that including diverse expert voices will improve outcomes and help to bridge gaps between technical and policy practitioners. Senior government officials, nonprofit and private sector experts, security researchers, hackers, academics and technologists from around the world all come together at Policy @ DEF CON.

Links:

Mastodon (defcon.social) - https://defcon.social/@defconpolicy
Website - https://defcon.org/policy/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248899
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248898
Twitter (@defconpolicy) - https://twitter.com/defconpolicy

Return to Index

PSV - Physical Security Village

PSV Village: Talk List
Home Page: https://www.physsec.org/
DC Village Page: #psv
DC Forums Page: https://forum.defcon.org/node/248895
DC Discord Chan: https://discord.com/channels/708208267699945503/732732893830447175
Location: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map
Social Media Links:
TW @physsec
TI @bypassvillage
LI @physsec
https://defcon.social/@physsec

The Physical Security Village explores the world of door hardware bypasses and techniques generally outside of the realm of cyber-security and lockpicking. Come learn some of these lock bypasses, how to fix them, and have the opportunity to try them out for yourself.

We'll be covering the basics, like the under-the-door-tool and latch slipping attacks, as well as an in depth look at more complicated bypasses. Learn about elevator hacking, defeating alarm systems and surveillance cameras, and cut-away and display models of common hardware to show how it works on the inside.

We are one of the easiest villages to get started in - read the instruction sheets we have or scan a QR code to learn the techniques, or ask any of our volunteers in the green shirts if you have questions! Looking for a challenge? Show us you can use lock bypass to escape from a pair of standard handcuffs in under 30 seconds and receive a prize!

Links:

Mastodon (defcon.social) - https://defcon.social/@physsec
Website - https://physsec.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248896
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248895

Return to Index

PWV - Password Village

PWV Village: Talk List
Home Page: https://passwordvillage.org/
DC Forums Page:
DC Discord Chan: https://discord.com/channels/708208267699945503/732733760742621214
Social Media Links:
TW @PasswordVillage
TI @passwordvillage
YT link

Return to Index

PYV - Payment Village

PYV Village: Talk List
Home Page: https://www.paymentvillage.org/
Sched Page: https://www.paymentvillage.org/workshops
DC Village Page: #payment
DC Forums Page: https://forum.defcon.org/node/248892
DC Discord Chan: https://discord.com/channels/708208267699945503/732733473558626314
Location: LVCC West/Floor 2/W202 - Map
Social Media Links:
TW @paymentvillage
TI @paymentvillage
YT link
https://t.me/paymentvillage

Come to the Payment Village to learn about payment technologies, their history, and how hackers bypass security and fraud mechanisms to cash out! Payment technologies play a crucial role in our daily lives, yet many of us lack an understanding of how they work. We invite you to explore the history of payments and to learn how modern-day payments work. The village is jam-packed with hands-on experiences and exciting challenges!

Unsure where to start? Sign up for one of our workshops to get going. Do you have adept problem-solving skills? Pick up a Payment Village credit card and take part in our card hacking challenge! Looking for a unique challenge and want to get physical? Try our scavenger hunt. Bigger and better than last year! Try your hand at our cash-grab machines with real money. Catch as much money as you can to decipher the clues and solve the challenges.

Links:

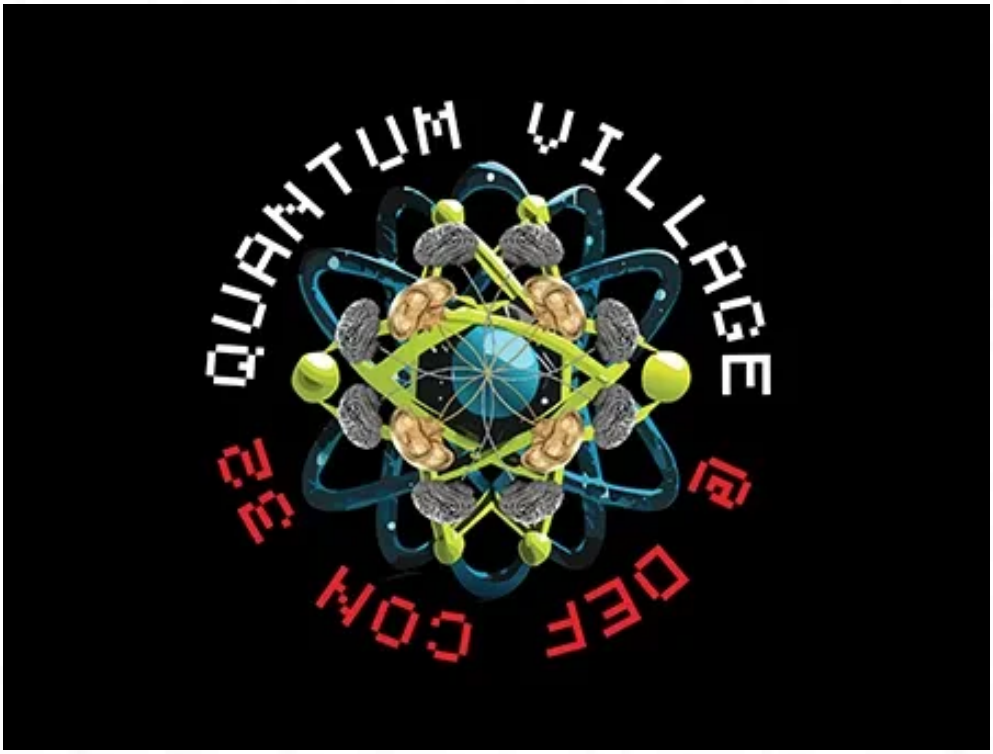
Website - https://www.paymentvillage.org/
YouTube - https://www.youtube.com/c/PaymentVillage
Telegram - https://t.me/paymentvillage
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248893
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248892
Twitter (@paymentvillage) - https://twitter.com/paymentvillage

---

Return to Index

QTV - Quantum Village

QTV Village: Talk List
Home Page: https://quantumvillage.org/
DC Village Page: #quantum
DC Forums Page: https://forum.defcon.org/node/248901
Location: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map
Social Media Links:
TW @quantum_village
DC https://discord.gg/6WUjH5cBXu
LI @quantumvillage
YT https://youtube.com/@quantum_village/



Attention Quantum Hackers - Quantum Village is Back for DEF CON 32! Come and explore and discover new technologies to hack - this year, we are focusing on quantum tech and society; from how to hack quantum networks to how 'thinking quantum' could change the world. We have a plethora of new activities, open to all levels, for hackers to come and learn quantum technologies - workshops, some talks, interactive demonstrations, and real quantum hardware! We also have the return of our infamous Quantum-CTF - pitch your wits against the Quantum Quizmasters and earn points for glory! Come and learn more about this exciting emerging field of technology and science, and become a QUANTUM HACKER!

We are very excited to bring back Quantum Village after our standing-room only success these last two years! This year we want to focus on looking at the parallels between how classical computing developed and became distributed and interconnected through LANs and WANs and later social networks, and how quantum computing is looking to do the same with the 'quantum internet', and what it means to have a 'social quantum network'. To this end we are working with some quantum infrastructure companies to have a real quantum network present at the event and ready for people to hack, e.g. via messing with the fibre lines we plan on distributing throughout the village.

We also want to use this analogy to get participants to ask questions about how quantum technologies can, should, and may fit into society at large, building on our 'Quantum Life' sessions in previous years that have lead to some really engaging discussions and thought provoking debates - all of which we would continue to build upon.

We also want to provide a bigger, more expansive Quantum CTF competition within the village that we would like to build our own hardware (e.g. badges) to present both as part of the challenge.

Links:

Website - https://quantumvillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248902
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248901
Twitter (@quantum_village) - https://twitter.com/quantum_village

---

Return to Index

RCV - Recon Village

RCV Village: Talk List
Home Page: https://www.reconvillage.org/
Sched Page: https://www.reconvillage.org/talks
DC Village Page: #recon
DC Forums Page: https://forum.defcon.org/node/248907
DC Discord Chan: https://discord.com/channels/708208267699945503/732733566051418193
Location: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map
Social Media Links:
TW @ReconVillage
FB @reconvillage
YT https://www.youtube.com/reconvillage/

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, CTFs, etc., with a common focus on Reconnaissance. The core objective of this village is to spread awareness about the importance of reconnaissance and open-source intelligence (OSINT) and demonstrate how even a small piece of information about a target can cause catastrophic damage to individuals and organizations. As recon is a vital phase for infosec as well as investigations, folks should have this skill set in their arsenal. People should check out Recon Village, as they get to learn novel point/recon techniques, play hands-on CTF, participate in Live Recon, and, most of all, have fun. At RV, we keep things simple, and the focus is on generating quality content using talks, workshops, CTF, live hacking, hackathons, etc. This year, we are launching a new hands-on event, i.e. Live Recon Contest, where we will challenge participants to perform recon on organization (pre-approved) - live and compete against each other to find as many as recon flags. This will include gauging skills like domain discovery, subdomain enumerations, GitHub Dorking, Metadata Extraction, data harvesting, social media profiling, threat intel mining, correlations and aggregations, and a lot more.

Also, to reduce the barrier to entry, we are going to host 101 Hands-on OSINT & Recon Workshops where people can learn and practice some new skills.

Similar to the previous years, there will be Awesome rewards for the winners, along with free t-shirts, stickers, village coins, and other schwag which attendees can grab and show off. We will be making changes to our badge as well. P.S. We will not be selling it, though.

Links:

Website - https://reconvillage.org/
YouTube - https://www.youtube.com/reconvillage
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248908
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248907
Twitter (@reconvillage) - https://twitter.com/reconvillage

Return to Index

RFV - Radio Frequency Village

RFV Village: Talk List
Home Page: https://rfhackers.com/
DC Village Page: #rfv
DC Forums Page: https://forum.defcon.org/node/248904
DC Discord Chan: https://discord.com/channels/708208267699945503/732732595493666826
Location: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map
Social Media Links:
TW @rfhackers
TW @rf_ctf
link
DC https://discordapp.com/invite/JjPQhKy

After 17 years of evolution, from the WiFi Village, to the Wireless Village, RF Hackers Sanctuary presents: The Radio Frequency Village at DEFCON 32. The Radio Frequency Village is an environment where people come to learn about the security of radio frequency (RF) transmissions, which includes wireless technology, applications of software defined radio (SDR), Bluetooth (BT), Zigbee, WiFi, Z-wave, Radio Frequency Identification (RFID), Infrared (IR) and other protocols within the usable RF spectrum. As a security community we have grown beyond WiFi, and even beyond Bluetooth and Zigbee. The RF Village includes talks on all manner of radio frequency command and control as well as communication systems. While everyone knows about the WiFi and Bluetooth attack surfaces, most of us rely on many additional technologies every day. RF Hackers Sanctuary is supported by a group of experts in the area of information security as it relates to RF technologies. RF Hackers Sanctuary's common purpose is to provide an environment in which participants may

explore these technologies with a focus on improving their skills through offense and defense. These learning environments are provided in the form of guest speakers, panels, and Radio Frequency Capture the Flag games, to promote learning on cutting edge topics as it relates to radio communications. We promise to still provide free WiFi.

Co-located with the RF Village is the RF Capture the Flag. Come for the talks, stay for the practice and the competition.

Who runs this thing?

RF Hackers Sanctuary is a group of all volunteers with expertise in radio security and various other related fields. We are the original creators of the WiFi Capture the Flag, Wireless Capture the Flag, and RF Capture the Flag. We are the original founders of the WiFi Village, Wireless Village, and RF Village. Often imitated, never duplicated.

Links:

Website - https://rfhackers.com/
Discord - https://discordapp.com/invite/JjPQhKy
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248905
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248904
Twitter (@rfhackers) - https://twitter.com/rfhackers
Twitter (@rf_ctf) - https://twitter.com/rf_ctf

Return to Index

RTV - Red Team Village

RTV Village: Talk List
Home Page: https://redteamvillage.io/
Sched Page: https://redteamvillage.io/schedule.html
DC Village Page: #redteam
DC Forums Page: https://forum.defcon.org/node/248910
Location: LVCC West/Floor 2/W204-W207 - Map
Social Media Links:
TW @RedTeamVillage_
YT https://www.youtube.com/redteamvillage
TI @redteamvillage
DC https://discord.gg/redteamvillage

The Red Team Village is focused on training the art of critical thinking, collaboration, and strategy in offensive security. The RTV brings together information security professionals to share new tactics and techniques in offensive security. Attendees may spend all three days engaged in introductory workshops or challenge themselves in an immersive Capture the Flag competition to put their newly obtained skills to the test.

Links:

Website - https://redteamvillage.io/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248911
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248910
Twitter (@RedTeamVillage_) - https://twitter.com/RedTeamVillage_

Return to Index

SEV - Social Engineering Village

SEV Village: Talk List
Home Page: https://www.se.community/
Sched Page: https://www.se.community/schedule/
DC Village Page: #sev
DC Forums Page: https://forum.defcon.org/node/248913
DC Discord Chan: https://discord.com/channels/708208267699945503/732733952867172382
Location: LVCC West/Floor 3/W317-W319 - Map
Social Media Links:
TW @sec_defcon
YT link
TI @se_community
LI @social-engineering-community
FB @Social-Engineering-Community-108883855139272

Hours
: Friday: 08:30 – 18:00 Saturday: 10:00 – 18:00 Sunday: 10:00 – 14:00

Location
: The Social Engineering Community Village will be in the LVCC West Hall rooms W317-319

Welcome to the Social Engineering Community! The SEC village focuses purely on the human aspect of security, Social Engineering, to enable people of all ages and backgrounds interested in the subject matter to have a venue to learn, discuss, and practice this craft.

This year, over three days at DEF CON, you can expect the following events to take place in the village:

- Vishing Competition (#SECVC): This edge-of-your-seat competition is where prior selected teams (who have already put WEEKS of work into the competition) place live phone calls inside a soundproof booth in front of SEC audience members to elicit as many objectives as possible. The highest score wins! This competition takes place only on Friday.
- Youth Challenge: Anyone 18 and under is invited to compete and learn about more than just Social Engineering; our challenges include areas in cryptography, network security, defusing intergalactic implosion bombs, and more. Can you stop the universe from imploding into what we're assuming is probably another universe but much smaller? We hope so! Otherwise, even the dolphins will have to find a new home.
- Cold Calls: This event lets DEF CON attendees sign up in the village (first come, first serve style) to place live phone calls inside the soundproof booth. We provide the target and phone number, then give a few objectives (easy, medium, and hard), and start a countdown timer to see if they have the skills to get information from a stranger with no preparation. There is nothing to prepare for, just bring yourself!
- New: This year, we may have a couple more surprises up our sleeves – stay tuned and check out our website as it gets closer to DEF CON with our daily schedule!

Links:

Website - https://www.se.community/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248914
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248913

Return to Index

SOC - Social Activities: Parties/Meetups

SOC Village: Talk List
DC Forums Page: https://forum.defcon.org/node/244769

Return to Index

TCV - Telecom Village

TCV Village: Talk List
Home Page: https://telecomvillage.com/
Sched Page: https://telecomvillage.com/index.html#program-details
DC Village Page: #telecom
DC Forums Page: https://forum.defcon.org/node/248918
Location: LVCC West/Floor 2/W201 - Map
Social Media Links:
TW @TelecomVillage

The Telecom Village is a platform for anyone with an interest in both the offensive and defensive facets of telecom security. The village is where a variety of events, including talks, CTFs, and discussions centred on telecom security, take place. The Telecom Village's primary focus would be on Telecom Security. We plan to host multiple hands-on events as part of the village to give participants an overview security specific challenges in a Telcom Network. This includes: CTFs in telecom signaling security and another one in Private 5G and select set of mini workshops and panels, spread across two days.

This Year we are planning to cover the following points Live4G/5G(SA) with Commercial BTS, internals and of a SIM Card, Simulating 4G/5G in a portal portable computing device, fundamentals of VoLTE/VoNR and its Attack vectors, MBSS for Telecom Security etc.

Telecom Security is an extremely focused and relatively closed domain within the Industry. We hope to bring this to a larger audience, ensure that they have a source which could act as a structure to facilitate learning and development in the sector. We will see larger adoption of Private 5G network across the globe and industries, which will come with it's own set of unique

challenges. We hope this village will play a key role is development and identification of key talents/projects which will help in tackling security challenges that plagues the telecom sector.

Links:

Website - https://telecomvillage.com/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248919
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248918
Twitter (@TelecomVillage) - https://twitter.com/TelecomVillage

---

Return to Index

TEV - Tamper Evident Village

TEV Village: Talk List
DC Village Page: #tev
DC Forums Page: https://forum.defcon.org/node/248916
Location: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. Tamper-evident technologies are often confused with "tamper resistant" or "tamper proof" technologies which attempt to prevent tampering in the first place. Referred to individually as "seals," many tamper technologies are easy to destroy, but a destroyed (or missing) seal would provide evidence of tampering! The goal of the TEV is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

The Tamper-Evident Village includes the following contests and events:

- The Box; an electronic tamper challenge. An extremely realistic explosive with traps, alarms, and a timer ticking down. One mistake and BOOM, you're dead. Make every second count! Sign ups on-site when the TEV begins.
- Tamper-Evident King of the Hill; a full-featured tamper challenge. Tamper single items at your leisure and attempt to beat the current best. There can be only ONE! No sign ups required, play on-site when the TEV begins.
- Badge Counterfeiting Contest; submit your best forgery of a DEF CON human badge. Other target badges are also available for those looking for more counterfeit fun!
- For your viewing pleasure, collections of high-security tamper-evident seals from around the world.
- Presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.
- Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags.

Links:

Discuss (DEF CON Forums) - https://forum.defcon.org/node/248917
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248916

Return to Index

VMV - Voting Village

VMV Village: Talk List
Home Page: https://votingvillage.org/
DC Village Page: #voting
DC Forums Page: https://forum.defcon.org/node/248921
DC Discord Chan: https://discord.com/channels/708208267699945503/732733881148506164
Location: LVCC West/Floor 2/W223-W224 - Map
Social Media Links:

TW @votingvillagedc
YT link
TI @votingvillagedc
LI @election-integrity-foundation
IG @votingvillage?igsh=MWJreTh6dGl3eDEzNg==

The Voting Village is an interactive educational environment that provides the public with the unique opportunity to have hands-on experience with our current election infrastructure. Attendees will be able to interact with multiple different types of voting systems, all of which are currently in use across the country today. Hackers will have the opportunity to test how secure these voting systems truly are, and will report to the Voting Village Lead's any vulnerabilities they find. The Voting Village explores all aspects of election security and works to promote a more secure democracy.

Attendees of Voting Village will also have access to Harri Hursti, the world's premier hacker and leading election and cyber security expert who has successfully hacked voting machines on multiple occasions. Aside from Harri, attendees will have access to other experts as well as the option of joining us for our speaker track (TALKS) that will take place every day except for the last Sunday of DEF CON. Our speaker track represents the most relevant government agencies and the top media outlets. Additionally, there will be multiple showings of Harri's HBO documentary, Kill Chain: The Cyber War on America's Elections. We will also have two Capture The Flags (CONTESTS) taking place throughout DEF CON.

Due to it being a presidential election year, the focus on elections is going to be extremely heightened. Having an open research environment like the Voting Village helps offset the misinformation and disinformation that is rampant leading up to a presidential election. The Voting Village not only addresses election infrastructure related issues but also focuses on information integrity as a critical element of our election system. Our talks given by the most reputable subject matter experts cover all of these election related topics.

Links:

Website - https://votingvillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248922
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248921
Twitter (@VotingVillageDC) - https://twitter.com/VotingVillageDC

Return to Index

WS - DEF CON Workshops

WS Village: Talk List
Home Page: https://defcon.org/html/defcon-32/dc-32-workshops.html
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_WS

Return to Index

XRV - XR Village

XRV Village: Talk List
Home Page: https://xrvillage.org/
DC Village Page: #xrv
DC Forums Page: https://forum.defcon.org/node/248924
Location: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map
Social Media Links:
TW @XRVillage
LI @xr-village
https://defcon.social/@xrvillage

Talks, playground for using XR tech, open bug hunt, bug bounty workshop, tech & art performances, VR gaming, and cross conference AR “Pokemon Go!” style collection experience. Federal agencies CISA and national laboratories Idaho & Pacific Northwest will be hosting interactive demos and an escape room in our space. They will be in collaboration with the ICS Village.

Workshop / Open Bug Hunt Pwn-a-Palooza (Collab with Hardware Hacking Village, Red Team Village)

The event is an open bug hunt with components of hardware hacking, XR rooted devices for workshop tie-in (VR headsets, glasses) and we are working with other villages and seeking support from industry pros to better direct the expectation of the hunt. We would like to offer prizing.

Playground

Open area for exploring emerging and existing XR tech; gaming, haptics, deconstructed devices to play with.

AR hunt / collection game

Collect village “stickers” throughout the con a la Pokemon Go! Style AR overlay that interacts with all the other villages at DEF CON. Think red mowhawks from Red Team Village, a viking from Adversary Village, a goat from OWASP, etc.

Links:

Mastodon (defcon.social) - https://defcon.social/xrvillage
Website - https://www.xrvillage.org/
Discuss (DEF CON Forums) - https://forum.defcon.org/node/248925
Sub-forum (DEF CON Forums) - https://forum.defcon.org/node/248924

Return to Index

Talk/Event Schedule

Thursday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Thursday - 05:00 PDT

Return to Index - Locations Legend

MISC - Defcon.run -

Thursday - 06:00 PDT

Return to Index - Locations Legend

MISC - cont...(05:00-07:59 PDT) - Defcon.run -

Thursday - 07:00 PDT

Return to Index - Locations Legend

MISC - Lost & Found -
MISC - cont...(05:00-07:59 PDT) - Defcon.run -

Thursday - 08:00 PDT

Return to Index - Locations Legend

MISC - Human Registration Open -
MISC - Merch (formerly swag) Area Open -- README -

Thursday - 09:00 PDT

Return to Index - Locations Legend

MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
WS - Sold Out - Offensive SCCM: Abusing Microsoft's C2 Framework - Chris Thompson,Duane Michael,Garrett Foster
WS - Sold Out - Med Team vs Red Team: Intro into Medical Device Hacking - Alex Delifer,Michael "v3ga" Aguilar
WS - Sold Out - Supercharge SAST: Semgrep Strategies for Secure Software - Arjun Gopalakrishna,Gautam Peri,Marcelo Ribeiro
WS - Sold Out - Dissecting Malware for Defense - Crafting Custom Yara Rules - Francisco Perdomo,Josh Stroschein
WS - Sold Out - Tracing The Pain Away - Practical Binary Tracing Techniques For Defeating Modern Malware Protections - Sean ,Serrgei Frankoff

Thursday - 10:00 PDT

Return to Index - Locations Legend

HDA - HDA Community - Open for Accessibility Questions/Help -
HRV - Ham in a Day Class - Dan "dan_kb6nu" Romanchik
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
WS - cont...(09:00-12:59 PDT) - Sold Out - Offensive SCCM: Abusing Microsoft's C2 Framework - Chris Thompson,Duane Michael,Garrett Foster
WS - cont...(09:00-12:59 PDT) - Sold Out - Med Team vs Red Team: Intro into Medical Device Hacking - Alex Delifer,Michael "v3ga" Aguilar
WS - cont...(09:00-12:59 PDT) - Sold Out - Supercharge SAST: Semgrep Strategies for Secure Software - Arjun Gopalakrishna,Gautam Peri,Marcelo Ribeiro
WS - cont...(09:00-12:59 PDT) - Sold Out - Dissecting Malware for Defense - Crafting Custom Yara Rules - Francisco Perdomo,Josh Stroschein
WS - cont...(09:00-12:59 PDT) - Sold Out - Tracing The Pain Away - Practical Binary Tracing Techniques For Defeating Modern Malware Protections - Sean ,Serrgei Frankoff

Thursday - 11:00 PDT

Return to Index - Locations Legend

HDA - cont...(10:00-17:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-16:59 PDT) - Ham in a Day Class - Dan "dan_kb6nu" Romanchik
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
WS - cont...(09:00-12:59 PDT) - Sold Out - Offensive SCCM: Abusing Microsoft's C2 Framework - Chris Thompson,Duane Michael,Garrett Foster
WS - cont...(09:00-12:59 PDT) - Sold Out - Med Team vs Red Team: Intro into Medical Device Hacking - Alex Delifer,Michael "v3ga" Aguilar
WS - cont...(09:00-12:59 PDT) - Sold Out - Supercharge SAST: Semgrep Strategies for Secure Software - Arjun Gopalakrishna,Gautam Peri,Marcelo Ribeiro
WS - cont...(09:00-12:59 PDT) - Sold Out - Dissecting Malware for Defense - Crafting Custom Yara Rules - Francisco Perdomo,Josh Stroschein
WS - cont...(09:00-12:59 PDT) - Sold Out - Tracing The Pain Away - Practical Binary Tracing Techniques For Defeating Modern Malware Protections - Sean ,Serrgei Frankoff

Thursday - 12:00 PDT

Return to Index - Locations Legend

CON - Hac-Man -
HDA - cont...(10:00-17:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-16:59 PDT) - Ham in a Day Class - Dan "dan_kb6nu" Romanchik
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
SOC - Friends of Bill W -
WS - cont...(09:00-12:59 PDT) - Sold Out - Offensive SCCM: Abusing Microsoft's C2 Framework - Chris Thompson,Duane Michael,Garrett Foster
WS - cont...(09:00-12:59 PDT) - Sold Out - Med Team vs Red Team: Intro into Medical Device Hacking - Alex Delifer,Michael "v3ga" Aguilar
WS - cont...(09:00-12:59 PDT) - Sold Out - Supercharge SAST: Semgrep Strategies for Secure Software - Arjun Gopalakrishna,Gautam Peri,Marcelo Ribeiro
WS - cont...(09:00-12:59 PDT) - Sold Out - Dissecting Malware for Defense - Crafting Custom Yara Rules - Francisco Perdomo,Josh Stroschein
WS - cont...(09:00-12:59 PDT) - Sold Out - Tracing The Pain Away - Practical Binary Tracing Techniques For Defeating Modern Malware Protections - Sean ,Serrgei Frankoff

Thursday - 13:00 PDT

Return to Index - Locations Legend

HDA - cont...(10:00-17:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-16:59 PDT) - Ham in a Day Class - Dan "dan_kb6nu" Romanchik
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -

Thursday - 14:00 PDT

Return to Index - Locations Legend

HDA - cont...(10:00-17:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-16:59 PDT) - Ham in a Day Class - Dan "dan_kb6nu" Romanchik
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
WS - Sold Out - Flipping the Coin: Red and Blue Teaming in Windows Environments (++) - Angus Strom,Troy Defty
WS - Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming - Jake “Hubble” Krasnov,Kevin "Kent" Clark,Rey "Privesc" Bango
WS - Sold Out - 64-bit Intel Assembly Language Programming for Hackers - Wesley McGrew
WS - Sold Out - Dodging the EDR Bullet: A Workshop on Malware Stealth Tactics - Dimitri Di Cristofaro,Giorgio "gbyolo" Bernardinetti
WS - Sold Out - Hide your kids, turn off your Wi-Fi, they Rogue APing up in here; 201 - James Hawk

Thursday - 15:00 PDT

Return to Index - Locations Legend

HDA - cont...(10:00-17:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-16:59 PDT) - Ham in a Day Class - Dan "dan_kb6nu" Romanchik
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Toxic BBQ -
WS - cont...(14:00-17:59 PDT) - Sold Out - Flipping the Coin: Red and Blue Teaming in Windows Environments (++) - Angus Strom,Troy Defty
WS - cont...(14:00-17:59 PDT) - Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming - Jake “Hubble” Krasnov,Kevin "Kent" Clark,Rey "Privesc" Bango
WS - cont...(14:00-17:59 PDT) - Sold Out - 64-bit Intel Assembly Language Programming for Hackers - Wesley McGrew
WS - cont...(14:00-17:59 PDT) - Sold Out - Dodging the EDR Bullet: A Workshop on Malware Stealth Tactics - Dimitri Di Cristofaro,Giorgio "gbyolo" Bernardinetti
WS - cont...(14:00-17:59 PDT) - Sold Out - Hide your kids, turn off your Wi-Fi, they Rogue APing up in here; 201 - James Hawk

Thursday - 16:00 PDT

Return to Index - Locations Legend

DDV - DDV starts accepting drives for duplication -
HDA - cont...(10:00-17:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-16:59 PDT) - Ham in a Day Class - Dan "dan_kb6nu" Romanchik
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - cont...(15:00-20:59 PDT) - Toxic BBQ -
SOC - QueerCon Mixer -
WS - cont...(14:00-17:59 PDT) - Sold Out - Flipping the Coin: Red and Blue Teaming in Windows Environments (++) - Angus Strom,Troy Defty
WS - cont...(14:00-17:59 PDT) - Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming - Jake “Hubble” Krasnov,Kevin "Kent" Clark,Rey "Privesc" Bango
WS - cont...(14:00-17:59 PDT) - Sold Out - 64-bit Intel Assembly Language Programming for Hackers - Wesley McGrew
WS - cont...(14:00-17:59 PDT) - Sold Out - Dodging the EDR Bullet: A Workshop on Malware Stealth Tactics - Dimitri Di Cristofaro,Giorgio "gbyolo" Bernardinetti
WS - cont...(14:00-17:59 PDT) - Sold Out - Hide your kids, turn off your Wi-Fi, they Rogue APing up in here; 201 - James Hawk

Thursday - 17:00 PDT

Return to Index - Locations Legend

DDV - cont...(16:00-19:59 PDT) - DDV starts accepting drives for duplication -
HDA - cont...(10:00-17:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - cont...(15:00-20:59 PDT) - Toxic BBQ -
SOC - cont...(16:00-17:59 PDT) - QueerCon Mixer -
SOC - Friends of Bill W -
WS - cont...(14:00-17:59 PDT) - Sold Out - Flipping the Coin: Red and Blue Teaming in Windows Environments (++) - Angus Strom,Troy Defty
WS - cont...(14:00-17:59 PDT) - Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming - Jake “Hubble” Krasnov,Kevin "Kent" Clark,Rey "Privesc" Bango
WS - cont...(14:00-17:59 PDT) - Sold Out - 64-bit Intel Assembly Language Programming for Hackers - Wesley McGrew
WS - cont...(14:00-17:59 PDT) - Sold Out - Dodging the EDR Bullet: A Workshop on Malware Stealth Tactics - Dimitri Di Cristofaro,Giorgio "gbyolo" Bernardinetti
WS - cont...(14:00-17:59 PDT) - Sold Out - Hide your kids, turn off your Wi-Fi, they Rogue APing up in here; 201 - James Hawk

Thursday - 18:00 PDT

Return to Index - Locations Legend

DDV - cont...(16:00-19:59 PDT) - DDV starts accepting drives for duplication -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(15:00-20:59 PDT) - Toxic BBQ -

Thursday - 19:00 PDT

Return to Index - Locations Legend

DDV - cont...(16:00-19:59 PDT) - DDV starts accepting drives for duplication -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(15:00-20:59 PDT) - Toxic BBQ -
SOC - DC702 -

Thursday - 20:00 PDT

Return to Index - Locations Legend

MISC - cont...(15:00-20:59 PDT) - Toxic BBQ -
SOC - Music Set / Entertainment (Cyberpunk Bar Thursday, ACK Stage) - Talk Sinn,Stitcharoo,Relay,deaddoll,CaptHz,Acid-T
SOC - Music Set / Entertainment (Thursday, SYN Stage) - PatAttack,Grind613,DotOrNot,DJ Vulp,Daemon Chadeau,CTRL / rsm
SOC - cont...(19:00-20:59 PDT) - DC702 -

Friday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Friday - 05:00 PDT

Return to Index - Locations Legend

MISC - Defcon.run -

Friday - 06:00 PDT

Return to Index - Locations Legend

MISC - cont...(05:00-07:59 PDT) - Defcon.run -
MISC - CycleOverride DEF CON Bike Ride -

Friday - 07:00 PDT

Return to Index - Locations Legend

MISC - cont...(05:00-07:59 PDT) - Defcon.run -

Friday - 08:00 PDT

Return to Index - Locations Legend

MISC - Human Registration Open -
MISC - Merch (formerly swag) Area Open -- README -
MISC - Lost & Found -
MISC - (08:15-10:30 PDT) - ISSCON -
SEV - (08:30-17:59 PDT) - Social Engineering Community Village Hours -

Friday - 09:00 PDT

Return to Index - Locations Legend

BICV - BIC United Kingdom Chapter Informational Virtual Opening Session - Ike Marizu
BICV - (09:30-09:59 PDT) - BIC Village Opening Q&A with Marcus Hutchins - Michaela Barnett,Marcus Hutchins
CON - Social Engineering Community Vishing Competition (SECVC) -
CON - Social Engineering Community Youth Challenge -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - cont...(08:15-10:30 PDT) - ISSCON -
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
WS - Sold Out - Traumatic Library Loading : If you want to use it, you have to implement it... - Yoann Dequeker
WS - Sold Out - Finding the Needle: An Introduction to Detection Engineering - Kathy Zhu,Troy Defty
WS - Sold Out - Whitebox Web Exploit Development - Cale Smith,Priyanka Joshi
WS - Sold Out - Small Choices, Global Repercussions: A Tabletop Exercise about Decision-Making in Healthcare Cybersecurity - Isabel Straw,Jorge Acevedo Canabal,Nathan Case
WS - Sold Out - Machine Learning for N00bs - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne

Friday - 10:00 PDT

Return to Index - Locations Legend

ADV - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - Adversary Village keynote kick-off panel - Abhijith “Abx” B R,Bryson Bort ,Ken Kato,Vivek Ramachandran,Sanne Maasakkers
AIV - AI Village Demos -
AIV - Opening Remarks - Sven Cattell,Lauren Putvin,Ravin Kumar
AIV - (10:30-11:30 PDT) - Generative Red Team 2 Kickoff - Sven Cattell,Will Pearce,Jerome Wynne,Sean McGregor,Nicole DeCario,Kent Wilson
APV - Fix the Flag Wargame - Harley Wilson
APV - (10:15-10:45 PDT) - Winning big: AppSec Considerations From the Casino Industry - Aleise McGowan,Tennisha Martin
ASV - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - PTP Flight Challenge - Pen Test Partners
ASV - Space Systems Security CTF – Platform Security - CT Cubed
ASV - Space Grand Challenge Luna - CalPoly
ASV - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - Selfie with a CubeSat - CalPoly
ASV - ARINC 664 CTF - Boeing
ASV - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - Drone Flying Experience - Dark Wolf
ASV - Drone Hacking Activity - Dark Wolf
ASV - Drone Capture the Flag (CTF) - Dark Wolf
ASV - Darkstar Badge Challenge - Lockheed Martin
ASV - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - Detect a Threat - TSA
ASV - CubeSat Simulator - AMSAT
ASV - Bricks in the Air -
ASV - (10:30-12:30 PDT) - Building the Ultimate Budget-Friendly Low Earth Orbit Satellite Ground Station - Victor Fernandez Minguillon
BBV - Caido Internals Deep-Dive - Emile Fugulin
BBV - Practical Exploitation of DoS in Bug Bounty - Roni "Lupin" Carta
BHV - Biohacking Village: Device Lab -
BICV - BIC Village Keynote: Cyber Threat Landscape And Law Enforcement - Kevin Parker
BTV - Building a Cyber Threat Intelligence Program from scratch for free! - Apurv Singh Gautam,Karan Dwivedi
BTV - Incident Response 101: Part 1 (IR Overview, Lifecycles, Frameworks, and Playbooks) - Jason Romero
BTV - (10:30-10:59 PDT) - Incident Response 101: Part 2 (Analyst Mindset and Quality Assurance) - David "CountZ3r0" Roman
CHV - Car Hacking Village Activities -
CLV - Opening Note -
CLV - Gone in 60 Seconds… How Azure AD/Entra ID Tenants are Compromised - Sean Metcalf
CLV - (10:50-11:30 PDT) - Catch them all! Detection Engineering and Purple Teaming in the Cloud - Christophe Tafani-Dereeper
CON - IoT Village CTF -
CON - Cloud Village CTF -
CON - Hardware Hacking Village CTF -
CON - Radio Frequency Capture the Flag -
CON - Embedded CTF -
CON - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -

CON - Biohacking Village CTF -
CON - QOLOSSUS -
CON - ICS CTF -
CON - Crash and Compile - Qualifications -
CON - Car Hacking Village CTF -
CON - HackFortress -
CON - Beverage Chilling Contraption Contest -
CON - Tinfoil Hat Contest -
CON - Chasse Partie Systems CTF -
CON - Gold Bug Challenge -
CON - CrackMeIfYouCan -
CON - DC's Next Top Threat Model (DCNTTM) -
CON - [CANCELED] AutoDriving CTF -
CON - Red Team Village CTF -
CON - Pinball High Score Contest -
CON - 5N4CK3Y Contest -
CON - Hac-Man -
CON - Darknet-NG -
CON - ? Cube -
CON - (10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - PhreakMe presented by HackedExistence -
CON - REALI7Y OVERRUN -
CON - Lonely Tag -
CON - Lonely Hard Drive -
CON - spyVspy -
CON - DEF CON Scavenger Hunt -
CON - Malware Contests: MARC I & BOMBE -
CON - Live Recon Contest in Progress -
CON - Adversary Wars CTF -
CON - HTB CTF: Data Dystopia -
CON - Octopus Game -
CON - Cyber Defender - The Game -
CON - CMD+CTRL at DEF CON 32 -
CON - Capture the Packet -
CON - HardWired -
CON - (10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(09:00-16:59 PDT) - Social Engineering Community Vishing Competition (SECVC) -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - It's In That Place Where I Put That Thing That Time -
CON - venator aurum - A Treasure Hunt -
CON - Radio Frequency Capture the Flag -
CON - [CANCELED] AutoDriving CTF -
CON - Cloud Village CTF -
CON - Gold Bug Challenge -
CPV - Differential privacy beyond algorithms: Challenges for successful deployment - Rachel Cummings
CPV - CPV: Day 1 Welcome -
DC - Welcome to DEF CON - Jeff "The Dark Tangent" Moss
DC - (10:30-11:15 PDT) - Spies and Bytes: Victory in the Digital Age - General Paul M. Nakasone
DC - Mobile Mesh RF Network Exploitation: Getting the Tea from goTenna - Erwin Karincic,Woody
DC - Where's the Money: Defeating ATM Disk Encryption - Matt Burch
DC - Securing CCTV Cameras Against Blind Spots - Jacob Shams
DC - (10:30-11:15 PDT) - Defeating magic by magic Using ALPC security features to compromise RPC services - WangJunJie Zhang,YiSheng He
DC - Behind Enemy Lines: Going undercover to breach the LockBit Ransomware Operation - Jon DiMaggio

DCG - DEF CON Groups - Open for questions and hanging out -
DDV - DDV open and accepting drives for duplication -
DL - Docker Exploitation Framework - Emmanuel Law,Rohit Pitke
DL - Zip It Up, Sneak It In - Introduction of apkInspector - Kaloyan Velikov,Leonidas Vasileiadis
DL - Volatile Vault - Data Exfiltration in 2024 - Moritz Laurin Thomas,Patrick Eisenschmidt
DL - Bluetooth Landscape Exploration & Enumeration Platform (BLEEP) - Paul Wortman
DL - Nebula - 3 Years of Kicking *aaS and Taking Usernames - Bleon Proko
DL - Cloud Offensive Breach and Risk Assessment (COBRA) - Anand Tiwari,Harsha Koushik
ESV - 101 Labs: Hardware Lab -
ESV - Hardware Hacking: Glitching Lab -
ESV - Secure Microcontroller Workshop -
ESV - 101 Labs: Firmware and Software exploitation -
ESV - Wireless & Networking workshop - Alex Kelly
ESV - Emulating (and Hacking) Embedded Devices -
HDA - HDA Community - Open for Accessibility Questions/Help -
ICSV - Does the World Need Another Threat Model, the Road to EMB3D - Niyo Little Thunder Pearson,Jack Cyprus,Wyatt Ford
ICSV - (10:30-10:59 PDT) - Attack and Defence in OT - Simulating attacks against hydroelectric power plants leveraging ICS Firing Ranges - Julia Dewitz-Würzelberger,Bernhard Sedlmayer,Sarah Mader
ICSV - Using ChatGPT to Write Defensive & Offensive Tools for ICS/OT - Mike Holcomb
IOTV - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - Hack My TV -
IOTV - Hardware Hacking GE Appliances -
IOTV - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - Safe Hacking -
IOTV - IoT Security at DEF CON 32 -
IOTV - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - Keysight CTF Challenge -
IOTV - IoT Village Hacking Playground -
IOTV - Phisherman's Wharf - Phishing for Beginners -
IOTV - Firmware Extraction and Analysis -
IOTV - (10:15-11:45 PDT) - IoT Cat Lamp - Kody K
LPV - Lockpicking Activities -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - All content areas generally open -
MISC - Vendors and Exhibitors Open -
MISC - Hard Hat Brigade - Community Space Open -
MISC - HHV Rube Goldberg Machine -
MISC - Robo Sumo -
MISC - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - WISP Community & Inclusion Room -
MISC - Welcome / Badge & Swag Pick Up -
MISC - Game Hacking Community Activities & CTF -
MISC - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - Show & Tell -
MISC - Retro Repair -
MISC - Dumb Terminal fun -
MISC - Small scale LAN party -
MISC - Egor's Keyboard Corner -
MISC - LHC's Unofficial Sticker Swap Table -
MISC - Lonely Hackers Club Community Room Open -
MISC - Resume Reviews -
MISC - LHC Meshtastic Activities and CTF -

MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Be Latino in Cybersecurity on markets outside LATAM - Salvador Mendonza,Lenin Alevski,Omar Santos,Alan Villaseñor,Guillermo Buendia
MISC - cont...(08:15-10:30 PDT) - ISSCON -
MISC - Open Events for DCNextGen -
PHV - Packet Inspector -
PHV - Packet Detective -
PHV - Botnets -
PHV - Linux Trainer -
PHV - Network-OS: Be The Cloud -
PHV - FleetDm -
PHV - Password lab -
PHV - Python + Packet Analysis + Machine Learning -
PHV - Regular Expressions (RegEx) Trainer -
PLV - US and International Public Cyber Policy 101 - Harley Geiger,Adam Dobell,Cassie Crossley
PSV - Physical Security Village Activities -
PYV - Payment Village CTF -
PYV - (10:15-10:20 PDT) - Introduction to Payment Village CTF - Leigh-Anne Galloway
QTV - QOLOSSUS: QUANTUM CTF CONTEST: How to get Started on The Quantum Capture The Flag -
QTV - Intro to Quantum with Q# - Mariia Mykhailova
RCV - Recon Village GE(O)SINT Challenge -
RCV - Bastardo Grande: Hunting the Largest Black Market Bike Fence In The World - Bryan Hance
RCV - (10:45-11:30 PDT) - Recursion is a Harsh Mistress: How (Not) To Build a Recursive Internet Scanner - TheTechromancer
RFV - Radio Frequency Village Events -
RFV - (10:30-11:25 PDT) - RF CTF Kick Off Day 1 - RF Hackers
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
TCV - Telecom Village Inauguration -
TEV - Tamper Evident Village Activities -
VMV - What is the Voting Village? - Catherine Terranova,Matt Blaze,Harri Hursti
VMV - (10:45-11:45 PDT) - Play by Play of the Curling v. Raffensperger Lawsuit - Susan Greenhalgh,Mary Kaiser,Drew Springall,Philip Stark
VMV - SIV Internet Voting Hacking Challenge - SIV
WS - cont...(09:00-12:59 PDT) - Sold Out - Traumatic Library Loading : If you want to use it, you have to implement it... - Yoann Dequeker
WS - cont...(09:00-12:59 PDT) - Sold Out - Finding the Needle: An Introduction to Detection Engineering - Kathy Zhu,Troy Defty
WS - cont...(09:00-12:59 PDT) - Sold Out - Whitebox Web Exploit Development - Cale Smith,Priyanka Joshi
WS - cont...(09:00-12:59 PDT) - Sold Out - Small Choices, Global Repercussions: A Tabletop Exercise about Decision-Making in Healthcare Cybersecurity - Isabel Straw,Jorge Acevedo Canabal,Nathan Case
WS - cont...(09:00-12:59 PDT) - Sold Out - Machine Learning for N00bs - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne
XRV - Pwning through the Metaverse - Quest Headset Vulnerability Research - Luke McLaren
XRV - ICS Village + XR Village Turn the lights on! -
XRV - Signals Are Everywhere -

Friday - 11:00 PDT

Return to Index - Locations Legend

ADV - (11:30-12:30 PDT) - Formidable Adversaries: Responding to Breaches, Ransomware, and State-Sponsored Threat Actors - Abhijith “Abx” B R,Adam "_whatshisface" Pennington,Ken Kato,Nikhil Mittal,Stryker
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - Modifying Impacket for Better OpSec - Ryan O'Donnell
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - cont...(10:30-11:30 PDT) - Generative Red Team 2 Kickoff - Sven Cattell,Will Pearce,Jerome Wynne,Sean McGregor,Nicole DeCario,Kent Wilson
AIV - (11:30-12:30 PDT) - BOLABuster: Harnessing LLMs for Automating BOLA Detection - Ravid Mazon,Jay Chen
AIxCC - (11:30-11:50 PDT) - SMOKE: Signature Management using Operational Knowledge and Environments - Tejas Patel
APV - Arsenal: AI Goat - Ofir Yakobi,Shir Sadon
APV - Arsenal: CyberChef like Automation within BurpSuite - Let's get cooking with the CSTC - Matthias Göhring,Florian Haag
APV - Mind-Controlling Other Applications: An intro to intra-process hacking - ILOVEPIE
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - Securing Frontends at Scale: Paving our Way to the Post-XSS World - Aaron Shim,jen-ozmen
APV - (11:45-12:15 PDT) - Ticking SQLi - Iggy
APV - Activity: Vulnerability Hunt - The Snippets Edition - Mário Leitão-Teixeira
APV - Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - mcdwayne
APV - Activity: Spot the Reachable by Backslash - Czesia Glik,Yossi Pik
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:30-12:30 PDT) - Building the Ultimate Budget-Friendly Low Earth Orbit Satellite Ground Station - Victor Fernandez Minguillon
ASV - An adversarial approach to Airline Revenue Management Proving Ground - Craig Lester
ASV - (11:30-11:59 PDT) - Aviation cybersecurity lightning talk: Three topics in thirty minutes - Ken Munro
BBV - Panel of Bug Bounty Community Leaders - Inti De Ceukelaire,Jessica Sexton,Ryan Rutan,Lucas Philippe,Michael "codingo" Skelton,Roni "Lupin" Carta
BBV - From Easy Wins to Epic Challenges: Bounty Hunter Edition - Daniel "Blaklis" Le Gall
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - (11:30-12:30 PDT) - From Redlining to Weblining: Examining Broadband Deserts and Racial Injustice - Dr. Fatou Sankare
BTV - cont...(10:00-11:30 PDT) - Building a Cyber Threat Intelligence Program from scratch for free! - Apurv Singh

Gautam,Karan Dwivedi
BTV - (11:45-13:30 PDT) - Adventures in Android Triage Collection - Omenscan
BTV - (11:15-12:15 PDT) - Cloud Native Security Platform for Defenders - Dafinga
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(10:50-11:30 PDT) - Catch them all! Detection Engineering and Purple Teaming in the Cloud - Christophe Tafani-Dereeper
CLV - (11:30-12:10 PDT) - The Oracle Awakens: Demystifying Privilege Escalation in the cloud - Felipe Pr0teus,Lucas Cioffi
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-14:59 PDT) - Crash and Compile - Qualifications -
CON - cont...(10:00-16:30 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-15:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC’s Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-17:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(09:00-16:59 PDT) - Social Engineering Community Vishing Competition (SECVC) -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -

CON - Betting on Your Digital Rights: 3rd Annual EFF Benefit Poker Tournament at DEF CON 32 -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-11:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-12:59 PDT) - Radio Frequency Capture the Flag -
CON - CrackMeIfYouCan -
CPV - Travel Better: Expedient Digital Defense - Grey Fox
DC - cont...(10:30-11:15 PDT) - Spies and Bytes: Victory in the Digital Age - General Paul M. Nakasone
DC - (11:30-11:59 PDT) - Atomic Honeypot: A MySQL Honeypot That Drops Shells - Alexander Rubin,Martin Rakhmanov
DC - No Symbols When Reversing? No Problem: Bring Your Own - Max "Libra" Kersten
DC - (11:30-12:15 PDT) - Listen to the whispers: web timing attacks that actually work - James "albinowax" Kettle
DC - cont...(10:30-11:15 PDT) - Defeating magic by magic Using ALPC security features to compromise RPC services - WangJunJie Zhang,YiSheng He
DC - (11:30-12:45 PDT) - High Intensity Deconstruction: Chronicles of a Cryptographic Heist - Babak Javadi,Aaron Levy,Nick Draffen
DC - (11:30-12:30 PDT) - Custom, cheap, easy, and safe badges - without starting from scratch - Joe "securelyfitz" FitzPatrick
DC - The XZ Backdoor Story: The Undercover Operation That Set the Internet on Fire - Thomas Roccia
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - cont...(10:00-11:45 PDT) - Docker Exploitation Framework - Emmanuel Law,Rohit Pitke
DL - cont...(10:00-11:45 PDT) - Zip It Up, Sneak It In - Introduction of apkInspector - Kaloyan Velikov,Leonidas Vasileiadis
DL - cont...(10:00-11:45 PDT) - Volatile Vault - Data Exfiltration in 2024 - Moritz Laurin Thomas,Patrick Eisenschmidt
DL - cont...(10:00-11:45 PDT) - Bluetooth Landscape Exploration & Enumeration Platform (BLEEP) - Paul Wortman
DL - cont...(10:00-11:45 PDT) - Nebula - 3 Years of Kicking *aaS and Taking Usernames - Bleon Proko
DL - cont...(10:00-11:45 PDT) - Cloud Offensive Breach and Risk Assessment (COBRA) - Anand Tiwari,Harsha Koushik
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - (11:30-12:30 PDT) - SSTV: How To Send Cat Memes Via Ham Radio - Hamster
ICSV - Importance of ICS knowledge from a engineer's perspective - Ray Baeza
ICSV - (11:30-11:55 PDT) - Invisible Invaders: Strategies to Combat Living Off the Land Techniques in ICS - Dan Gunter
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:15-11:45 PDT) - IoT Cat Lamp - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -

MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - Intro to Circuit Python (Badge class level 1) -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - (11:30-17:30 PDT) - Book Signings -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(10:00-12:59 PDT) - Resume Reviews -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Prendendo Fraudadores utilizando Técnicas de Red Team - Gustavo Roberto
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PLV - cont...(10:00-11:45 PDT) - US and International Public Cyber Policy 101 - Harley Geiger,Adam Dobell,Cassie Crossley
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - (11:30-12:40 PDT) - User Behaviour Analytics in Payments - Karthik Tadinada
QTV - cont...(10:05-11:25 PDT) - Intro to Quantum with Q# - Mariia Mykhailova
QTV - (11:25-12:15 PDT) - How do we make LLVM quantum? - Josh Isaac
RCV - cont...(10:00-13:59 PDT) - Recon Village GE(O)SINT Challenge -
RCV - cont...(10:45-11:30 PDT) - Recursion is a Harsh Mistress: How (Not) To Build a Recursive Internet Scanner - TheTechromancer
RCV - (11:30-12:05 PDT) - Hospitals, Airports, and Telcos — Modern Approach to Attributing Hacktivism Attacks - Itay Cohen
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(10:30-11:25 PDT) - RF CTF Kick Off Day 1 - RF Hackers
RFV - (11:30-12:25 PDT) - Software Defined Radio 101: Capturing Your First RFCTF Flag - bkobe
RTV - The Art of Critical Thinking through an Adversarial Mindset? (RTV Keynote) - Ben "NahamSec" Sadeghipour,YTCracker,Barrett "pwneip" Darnell,Ryan M. "0dayCTF" Montgomery,Savannah "lazzslayer" Lazzara
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
TCV - 5G Fortress - Akib Sayyed
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - cont...(10:45-11:45 PDT) - Play by Play of the Curling v. Raffensperger Lawsuit - Susan Greenhalgh,Mary Kaiser,Drew Springall,Philip Stark
VMV - (11:45-12:45 PDT) - How to Steal Voting Software and Get Away With It - Susan Greenhalgh,Anna Bower,Rich DeMillo,Marilyn Marks
VMV - cont...(10:00-12:59 PDT) - SIV Internet Voting Hacking Challenge - SIV
WS - cont...(09:00-12:59 PDT) - Sold Out - Traumatic Library Loading : If you want to use it, you have to implement it... -

Yoann Dequeker
WS - cont...(09:00-12:59 PDT) - Sold Out - Finding the Needle: An Introduction to Detection Engineering - Kathy Zhu,Troy Defty
WS - cont...(09:00-12:59 PDT) - Sold Out - Whitebox Web Exploit Development - Cale Smith,Priyanka Joshi
WS - cont...(09:00-12:59 PDT) - Sold Out - Small Choices, Global Repercussions: A Tabletop Exercise about Decision-Making in Healthcare Cybersecurity - Isabel Straw,Jorge Acevedo Canabal,Nathan Case
WS - cont...(09:00-12:59 PDT) - Sold Out - Machine Learning for N00bs - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne
XRV - National Labs Use of XR - Martin Pratt
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - Trip Through Reality XR for Performances Masterclass with the Glad Scientist - The Glad Scientist

Friday - 12:00 PDT

Return to Index - Locations Legend

ADV - cont...(11:30-12:30 PDT) - Formidable Adversaries: Responding to Breaches, Ransomware, and State-Sponsored Threat Actors - Abhijith “Abx” B R,Adam "_whatshisface" Pennington,Ken Kato,Nikhil Mittal,Stryker
ADV - (12:30-12:59 PDT) - MFT: Malicious Fungible Tokens - Cybelle Oliveira ,Mauro Eldritch
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(11:00-12:59 PDT) - Modifying Impacket for Better OpSec - Ryan O'Donnell
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - cont...(11:30-12:30 PDT) - BOLABuster: Harnessing LLMs for Automating BOLA Detection - Ravid Mazon,Jay Chen
APV - cont...(11:00-12:59 PDT) - Arsenal: AI Goat - Ofir Yakobi,Shir Sadon
APV - cont...(11:00-12:59 PDT) - Arsenal: CyberChef like Automation within BurpSuite - Let's get cooking with the CSTC - Matthias Göhring,Florian Haag
APV - cont...(11:00-13:59 PDT) - Mind-Controlling Other Applications: An intro to intra-process hacking - ILOVEPIE
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - cont...(11:45-12:15 PDT) - Ticking SQLi - Iggy
APV - (12:30-12:59 PDT) - Hacking Corporate Banking for Fun and Profit - Charles Waterhouse,Nikhil "niks" Shrivastava
APV - cont...(11:00-12:59 PDT) - Activity: Vulnerability Hunt - The Snippets Edition - Mário Leitão-Teixeira
APV - cont...(11:00-12:59 PDT) - Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - mcdwayne
APV - cont...(11:00-12:59 PDT) - Activity: Spot the Reachable by Backslash - Czesia Glik,Yossi Pik
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:30-12:30 PDT) - Building the Ultimate Budget-Friendly Low Earth Orbit Satellite Ground Station - Victor Fernandez Minguillon
BBV - cont...(11:00-12:15 PDT) - Panel of Bug Bounty Community Leaders - Inti De Ceukelaire,Jessica Sexton,Ryan Rutan,Lucas Philippe,Michael "codingo" Skelton,Roni "Lupin" Carta
BBV - (12:15-13:45 PDT) - A Zero to Hero Crash Course to Server-Side Request Forgery (SSRF) - Ben "NahamSec" Sadeghipour
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - cont...(11:30-12:30 PDT) - From Redlining to Weblining: Examining Broadband Deserts and Racial Injustice - Dr. Fatou Sankare
BTV - cont...(11:45-13:30 PDT) - Adventures in Android Triage Collection - Omenscan
BTV - cont...(11:15-12:15 PDT) - Cloud Native Security Platform for Defenders - Dafinga
BTV - (12:30-13:30 PDT) - Stealer Logs: Automation, Analysis, & Espionage in the World's Most Interesting Dataset - Eric

Clay,Nick Ascoli
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(11:30-12:10 PDT) - The Oracle Awakens: Demystifying Privilege Escalation in the cloud - Felipe Pr0teus,Lucas Cioffi
CLV - One Port to Serve Them All - Google GCP Cloud Shell Abuse - Hubert Lin
CLV - (12:30-12:59 PDT) - Cloud Offensive Breach and Risk Assessment (COBRA) - Harsha Koushik,Anand Tiwari
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - Gold Bug: Welcome -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-14:59 PDT) - Crash and Compile - Qualifications -
CON - cont...(10:00-16:30 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-15:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC’s Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-17:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - Red Alert ICS CTF -
CON - Aw, man…pages! -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - Blacks in Cyber CTF -
CON - Blacks in Cyber CTF -

CON - cont...(09:00-16:59 PDT) - Social Engineering Community Vishing Competition (SECVC) -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-12:59 PDT) - Radio Frequency Capture the Flag -
CON - Blacks in Cyber CTF -
CON - Blacks in Cyber CTF -
DC - Fireside Chat with DNSA Anne Neuberger - Anne Neuberger,Jeff "The Dark Tangent" Moss
DC - On Your Ocean's 11 Team, I'm the AI Guy (technically Girl) - Harriet Farlow
DC - cont...(11:30-12:15 PDT) - Listen to the whispers: web timing attacks that actually work - James "albinowax" Kettle
DC - (12:30-13:15 PDT) - Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access - Nick Frichette
DC - cont...(11:30-12:45 PDT) - High Intensity Deconstruction: Chronicles of a Cryptographic Heist - Babak Javadi,Aaron Levy,Nick Draffen
DC - cont...(11:30-12:30 PDT) - Custom, cheap, easy, and safe badges - without starting from scratch - Joe "securelyfitz" FitzPatrick
DC - Veilid Dev and Community Meetup - The_Gibson
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - distribRuted - Distributed Attack Framework - Ismail Melih Tas,Numan Ozdemir
DL - BypassIT - Using AutoIT & Similar Tools for Covert Payload Delivery - Ezra Woods,Mike Manrod
DL - Tengu Marauder - Leonardo Serrano,Lexie Thach
DL - Skynet - Craig Chamberlain,Rewanth Tammana
DL - The World Wide Paraweb - Nathan Sidles
DL - Serberus - Patrick Kiley
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(11:30-12:30 PDT) - SSTV: How To Send Cat Memes Via Ham Radio - Hamster
ICSV - A hole in one: pwning a cruise ship from a golf simulator and other tales of maritime IT-OT misconvergence - Andrew Tierney
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - Learn Beginner Soldering With the Meow Mixer Badge - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
LPV - Safecracking for Everyone - Jared Dygert
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -

MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(11:30-17:30 PDT) - Book Signings -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-12:59 PDT) - Resume Reviews -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Bridging the Gap: How the American Legion Provides Veterans with a Sense of Belonging and Support - Chris Davis
MISC - SQLi to Root Access: Exploiting a ISP infrastructure - Ignacio Daniel Navarro
MISC - (12:30-13:30 PDT) - Mexicans Together - Un vistazo a recientes investigaciones de nuestros dos equipos globales - Ashley Hiram M.,Isabel Manjarrez
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - The Curious Case of Alice and Bob: What You Can (And Cannot!) Do as Digital Investigators - Catherine J. Ullman
PLV - Rules All Hackers Must Follow in War - Dr. Kosuke Onishi
PSV - (12:30-12:59 PDT) - RFID 101 - Andrew M,Ege Feyzioglu
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - Flipping Locks (The Remix) - Remote Badge Cloning with the Flipper Zero and More - Langston Clement,Dan Goga
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - cont...(11:30-12:40 PDT) - User Behaviour Analytics in Payments - Karthik Tadinada
QTV - cont...(11:25-12:15 PDT) - How do we make LLVM quantum? - Josh Isaac
QTV - (12:15-12:59 PDT) - A Hacker's guide to PQC - Konstantinos Karagiannis
RCV - cont...(10:00-13:59 PDT) - Recon Village GE(O)SINT Challenge -
RCV - cont...(11:30-12:05 PDT) - Hospitals, Airports, and Telcos — Modern Approach to Attributing Hacktivism Attacks - Itay Cohen
RCV - Ask Me Anything - Daniel Cutberth, Moderated by Sudhanshu - Sudhanshu,Daniel Cuthbert
RCV - Bypassing WHOIS Rate Limiting and Alerting on Fresh Enterprise Domains - Willis Vandevanter
RCV - (12:40-13:25 PDT) - SWGRecon: Automate SWG Rules, Policy, and Bypass Enumeration - Vivek Ramachandran
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(11:30-12:25 PDT) - Software Defined Radio 101: Capturing Your First RFCTF Flag - bkobe
RFV - (12:30-13:25 PDT) - Exploiting insecure OTA updates to create the worlds first Toothbrush Botnet and selfreplicating ESP32 worm - Lozaning
RTV - Mining for Abandoned Gold in DNS - Matt Pawloski
RTV - Modern Red Teaming: macOS, K8s, and Cloud - Chris Gates,int eighty (of Dual Core)

RTV - Abusing DevOps to Pivot Between Cloud and On-Prem - Colbert Zhu,Tom Porter
RTV - Red Team Terraform Workshop - Moses Frost
RTV - Bypassing Corporate controls on Mac Devices - Adwiteeya Agrawal,Ian Foster
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
SOC - Friends of Bill W -
SOC - Veilid Dev and Community Meetup -
TCV - cont...(11:00-13:59 PDT) - 5G Fortress - Akib Sayyed
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - cont...(11:45-12:45 PDT) - How to Steal Voting Software and Get Away With It - Susan Greenhalgh,Anna Bower,Rich DeMillo,Marilyn Marks
VMV - cont...(10:00-12:59 PDT) - SIV Internet Voting Hacking Challenge - SIV
WS - cont...(09:00-12:59 PDT) - Sold Out - Traumatic Library Loading : If you want to use it, you have to implement it... - Yoann Dequeker
WS - cont...(09:00-12:59 PDT) - Sold Out - Finding the Needle: An Introduction to Detection Engineering - Kathy Zhu,Troy Defty
WS - cont...(09:00-12:59 PDT) - Sold Out - Whitebox Web Exploit Development - Cale Smith,Priyanka Joshi
WS - cont...(09:00-12:59 PDT) - Sold Out - Small Choices, Global Repercussions: A Tabletop Exercise about Decision-Making in Healthcare Cybersecurity - Isabel Straw,Jorge Acevedo Canabal,Nathan Case
WS - cont...(09:00-12:59 PDT) - Sold Out - Machine Learning for N00bs - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - cont...(11:00-12:59 PDT) - Trip Through Reality XR for Performances Masterclass with the Glad Scientist - The Glad Scientist

Friday - 13:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - Introduction to MITRE Caldera Through Adversary Emulation - Rachel Murphy,Mark Perry
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - (13:30-14:30 PDT) - AI'll be watching you. Greybox Attacks against an Embedded AI - Ryan Tracey,Kasimir Schulz,Tom Boner
APV - Arsenal: GraphQL Armor - Open Source GraphQL Security - Antoine Carossio,Tristan Kalos
APV - cont...(11:00-13:59 PDT) - Mind-Controlling Other Applications: An intro to intra-process hacking - ILOVEPIE
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - (13:15-13:45 PDT) - SDLC Nightmares - Defeating Secure Code Review GPT Hallucinations - Wang Zhilong,Xinzhi Luo
APV - Activity: Capture the Container by Chainguard - Jonathan Leitschuh
APV - Q&A With OWASP -
APV - Activity: Test Your AppSec Knowledge by Deepfactor - Mike Larkin
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - BYOS – Bring Your Own Satellite - Tim Fowler
BBV - cont...(12:15-13:45 PDT) - A Zero to Hero Crash Course to Server-Side Request Forgery (SSRF) - Ben "NahamSec" Sadeghipour
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - Worried about AI taking your job? Then this talk is for you. - Levone Campbell
BTV - cont...(11:45-13:30 PDT) - Adventures in Android Triage Collection - Omenscan
BTV - cont...(12:30-13:30 PDT) - Stealer Logs: Automation, Analysis, & Espionage in the World's Most Interesting Dataset - Eric Clay,Nick Ascoli
CHV - V2GEvil: Ghost in the wires - Pavel Khunt,Thomas "Cr0wTom" Sermpinis
CHV - (13:30-13:59 PDT) - Building a secure and resilient nationwide EV charging network: the role of hackers in the clean energy revolution - Harry Krejsa,Sarah Hipel
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - ExploitIfNotExists: Privilege Escalation & Persistence with Azure Policy - Zander Mackie
CLV - (13:25-13:59 PDT) - Exploit K8S via Misconfiguration .YAML in CSP environments - Wooseok Kim,Changhyun Park
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -

CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-14:59 PDT) - Crash and Compile - Qualifications -
CON - cont...(10:00-16:30 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-15:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC’s Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(12:00-19:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-17:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - Hacking Boundary Terminal -
CON - cont...(12:00-16:59 PDT) - Red Alert ICS CTF -
CON - AI Art Battle -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(09:00-16:59 PDT) - Social Engineering Community Vishing Competition (SECVC) -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CPV - CPV: Intro to Cyphers -

CPV - (13:30-13:45 PDT) - Surprise Talk - Rachel Cummings
DC - If Existing Cyber Vulnerabilities Magically Disappeared Overnight, What Would Be Next? - Dr. Stefanie Tompkins,Dr. Renee Wegrzyn,Peiter “Mudge” Zatko
DC - Sshamble: Unexpected Exposures in the Secure Shell - HD Moore,Rob King
DC - cont...(12:30-13:15 PDT) - Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access - Nick Frichette
DC - (13:30-14:15 PDT) - Digital Emblems: When markings are required under international law, but you don’t have a rattle-can handy - Bill Woodcock
DC - Defeating EDR Evading Malware with Memory Forensics - Andrew Case,Austin Sellers,Golden Richard,David McDonald,Gustavo Moreira
DC - cont...(12:00-13:15 PDT) - Veilid Dev and Community Meetup - The_Gibson
DC - (13:30-14:15 PDT) - Xiaomi The Money - Our Toronto Pwn2Own Exploit and Behind The Scenes Story - Ken Gannon,Ilyes Beghdadi
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - cont...(12:00-13:45 PDT) - distribRuted - Distributed Attack Framework - Ismail Melih Tas,Numan Ozdemir
DL - cont...(12:00-13:45 PDT) - BypassIT - Using AutoIT & Similar Tools for Covert Payload Delivery - Ezra Woods,Mike Manrod
DL - cont...(12:00-13:45 PDT) - Tengu Marauder - Leonardo Serrano,Lexie Thach
DL - cont...(12:00-13:45 PDT) - Skynet - Craig Chamberlain,Rewanth Tammana
DL - cont...(12:00-13:45 PDT) - The World Wide Paraweb - Nathan Sidles
DL - cont...(12:00-13:45 PDT) - Serberus - Patrick Kiley
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - Ham Radio Exams -
ICSV - HandPwning: "Your Hand is your Passport. Verify me. Now let me in!" - Luca "CYBERANTANI" Bongiorni
ICSV - (13:30-13:55 PDT) - Cyber Informed Engineering for Critical Infrastructure - Aaron Crow
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(12:00-13:30 PDT) - Learn Beginner Soldering With the Meow Mixer Badge - Kody K
IOTV - Preparing for the Future: A Discussion of our Rapidly Evolving Threat Landscape - Jamie Hardy,Rachael Tubbs,Steve McGregory ,Ted Harrington
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
LPV - Safecracking Practical Demonstration - Jared Dygert
LPV - (13:30-13:59 PDT) - Doors, Cameras, & Mantraps: Oh my! - Dylan "The Magician" Baklor
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -

MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(11:30-17:30 PDT) - Book Signings -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - No CTF? No Problem! Leveraging Alternate Reality Games to Develop OSINT and Cryptography Skills - John "2PAC" Smithberger
MISC - cont...(12:30-13:30 PDT) - Mexicans Together - Un vistazo a recientes investigaciones de nuestros dos equipos globales - Ashley Hiram M.,Isabel Manjarrez
MISC - (13:30-13:59 PDT) - De Escudo a Espada: Cómo un Antivirus Facilitó el compromiso de una compañía - R4v3n Bl4ck
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - MoWireless MoProblems: Modular Wireless Survey Systems and the Data Analytics That Love Them - Geoff Horvath,Winson Tam
PHV - (13:30-14:30 PDT) - Signature-Based Detection Using Network Timing - Josh Pyorre
PLV - The Value of Trust in the Open-source Software Ecosystem - Nasreen Djouini,Jordan Kasper,Aeva Black
PSV - Bypass 101 - Karen Ng,Sam Mayers
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - (13:30-13:59 PDT) - Bogus Badges: The Art and Innovation of Badge Counterfeiting - Nick Warner
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - Attacking and defending card present transactions - Yurii Zadoianchuk,Stephan Viljoen,Sebastiaan Pierrot
RCV - cont...(10:00-13:59 PDT) - Recon Village GE(O)SINT Challenge -
RCV - cont...(12:40-13:25 PDT) - SWGRecon: Automate SWG Rules, Policy, and Bypass Enumeration - Vivek Ramachandran
RCV - Interview - Mika Devonshire, Hosted by Himanshu Das - Mika Devonshire,Himanshu Das
RCV - (13:25-13:59 PDT) - Tapping the OSINT potential of Telegram - Megan Squire
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(12:30-13:25 PDT) - Exploiting insecure OTA updates to create the worlds first Toothbrush Botnet and selfreplicating ESP32 worm - Lozaning
RFV - (13:30-14:25 PDT) - iCLASS - Throwing away the keys - Tiernan "nvx" Messmer
RTV - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - Red Goes Purple: Executing the Attack Path - Omar Santos,Graham Helton,Kevin "Kent" Clark
RTV - Adversary Simulation: Using Blue Eyes to See Red - Fred Wilmot,Sebastien Tricaud
RTV - Simulated Drone Hacking - Nick Aleks

RTV - Badge Cloning: A Penetration Tester's Guide to Capturing and Writing Badges - Travis Weathers,Ralph May
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
SOC - cont...(12:00-13:30 PDT) - Veilid Dev and Community Meetup -
TCV - cont...(11:00-13:59 PDT) - 5G Fortress - Akib Sayyed
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - Risk Limiting Audits From the Source - Philip Stark
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -

Friday - 14:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(13:00-14:59 PDT) - Introduction to MITRE Caldera Through Adversary Emulation - Rachel Murphy,Mark Perry
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - cont...(13:30-14:30 PDT) - AI'll be watching you. Greybox Attacks against an Embedded AI - Ryan Tracey,Kasimir Schulz,Tom Boner
AIV - (14:30-14:59 PDT) - Removing the Ring of Gyges: Lessons from Securing AI Systems Against File Format Abuse - Sean Oesch,Luke Koch,Brian Weber,Amul Chaulagain,Matthew Dixson,Jared Dixon,Cory Watson
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - Relative Path File Injection: The Next Evolution in RPO - Ian Hickey
APV - (14:45-15:15 PDT) - Threat Modeling in the Age of AI - Adam Shostack
APV - cont...(13:00-14:59 PDT) - Activity: Capture the Container by Chainguard - Jonathan Leitschuh
APV - cont...(13:00-14:59 PDT) - Q&A With OWASP -
APV - cont...(13:00-14:59 PDT) - Activity: Test Your AppSec Knowledge by Deepfactor - Mike Larkin
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(13:00-14:59 PDT) - BYOS – Bring Your Own Satellite - Tim Fowler
BBV - Why You Should Be Hunting on Web3 Bug Bounties - Gonçalo Marques Raposo de Magalhães
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - "BYOCTF" - Bring Your Own [Challenges||Capture] The Flag - Eli McRae
BTV - Area DC32: An Interactive Tabletop Takes Flight (A BTV Panel) - Aakin Patel,Caspian Kilkelly,Gwyddia,Harlan Geer,Shea Nangle,Matt Mayes
BTV - (14:30-15:30 PDT) - BTV Conversations: Exploring the Cyberpsychology of Cyber Defender Acceptance Behaviors and Personality Traits - Todd Fletcher
CHV - UDSonCAN Attacks: Discovering Safety-Critical Risks by Fuzzing - Jonghyuk Song,Seunghee Han,Soohwan Oh
CHV - (14:30-14:59 PDT) - How I discovered and hacked Learning Codes of the key job of a car assembled in my country - Danilo Erazo
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - UnOAuthorized: Discovering the path to privilege elevation to Global Administrator - Eric Woodruff
CLV - (14:30-15:10 PDT) - Attacking and Defending Software Supply Chains: How we got Admin in your Clouds! - Mike Ruth
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -

CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-14:59 PDT) - Crash and Compile - Qualifications -
CON - Hack3r Runw@y - Signups -
CON - cont...(10:00-16:30 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-15:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(12:00-19:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-17:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(12:00-16:59 PDT) - Red Alert ICS CTF -
CON - cont...(13:00-14:59 PDT) - AI Art Battle -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(09:00-16:59 PDT) - Social Engineering Community Vishing Competition (SECVC) -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -

CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CPV - Data Brokers and the Threat to Your Privacy - Yael Grauer
DC - DEF CON Unplugged: Cocktails & Cyber with Jeff & Jen - Jen Easterly
DC - Optical Espionage: Using Lasers to Hear Keystrokes Through Glass Windows - samy kamkar
DC - cont...(13:30-14:15 PDT) - Digital Emblems: When markings are required under international law, but you don't have a rattle-can handy - Bill Woodcock
DC - (14:30-15:15 PDT) - Breaching AWS Accounts Through Shadow Resources - Yakir Kadkoda,Michael Katchinskiy,Ofek Itach
DC - The Way To Android Root: Exploiting Your GPU On Smartphone - Xiling Gong,Eugene Rodionov,Xuan Xing
DC - cont...(13:30-14:15 PDT) - Xiaomi The Money - Our Toronto Pwn2Own Exploit and Behind The Scenes Story - Ken Gannon,Ilyes Beghdadi
DC - (14:30-15:15 PDT) - Joe and Bruno's Guide to Hacking Time: Regenerating Passwords from RoboForm's Password Generator - Joe "Kingpin" Grand,Bruno Krauss
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - Automated Control Validation with Tommyknocker - Jeremy Banker
DL - HIDe & SEEK - Jonathan Fischer,Matthew Richard
DL - SCAGoat - Exploiting Damn Vulnerable SCA Application - Hare Krishna Rai,Prashant Venkatesh
DL - Garak - Erick Galinkin,Leon Derczynski
DL - XenoboxX - Hardware Sandbox Toolkit - Cesare Pizzi
DL - Hopper - Distributed Fuzzer - Luciano Remes,Wade Cappa
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - HDA Presents : Naomi Brockwell - Naomi Brockwell
HRV - cont...(13:00-15:59 PDT) - Ham Radio Exams -
HRV - Hacking the Quansheng UV-K5 - Jon Marler
ICSV - The Risk and Reward of Distributed Industrial Control - Joe Slowik
ICSV - (14:30-14:59 PDT) - Mapping the Landscape: Top 10 Cybersecurity Trends in Critical Infrastructure for 2024 - Mars Cheng
ICSV - Detouring Danger: Hunting Privileged File Operation Vulnerabilities in OT/ICS software - Asher Davila
IOTV - (14:30-15:30 PDT) - Exploration of Cellular Based IoT Technology - Carlota Bindner,Deral Heiland
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - Solder your own cat shaped WiFi Haking tool - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
LPV - cont...(13:00-15:59 PDT) - Safecracking Practical Demonstration - Jared Dygert
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -

MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - Hard Hat Brigade Maker Panel -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - Friendship Bracelet Making -
MISC - Hack the Badge (Badge class level 2) -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(11:30-17:30 PDT) - Book Signings -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - Resume Reviews -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Book Signing: Visual Threat Intelligence: An Illustrated Guide for Threat Researchers - Thomas Roccia
MISC - Amenaza persistente: UXHIL y la propagación de URSA - Jesika Juarez,Armando Aguilar
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(13:30-14:30 PDT) - Signature-Based Detection Using Network Timing - Josh Pyorre
PLV - (14:30-15:15 PDT) - Human Dignity in AI and Tech Policy - Jan Trzaskowski
PLV - Advocating for an Inclusive Cyber-Civil Rights Policy Agenda for Vulnerable Communities - Nicole Tisdale,Kemba Walden,Jacob H Braun,Elizabeth Eigner
PSV - Physical Security Assessment Basics for Internal Employees - Billy Graydon
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - (14:30-15:30 PDT) - Your Smartcard is Dumb: A Brief History of Hacking Access Control Systems - Chad Shortman
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - (14:30-15:10 PDT) - Emulating Magstripe with Arduino - Leigh-Anne Galloway
QTV - Quantum on the flip side - A global south perspective on Quantum Technologies - Bruna Shinohara de Mendonça
RCV - ToolMakers Hackathon -
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(13:30-14:25 PDT) - iCLASS - Throwing away the keys - Tiernan "nvx" Messmer
RFV - (14:30-15:25 PDT) - Yet another way of exfiltrating data from air-gapped systems OR Oh no, everything is a radio - C$,Endeavors
RTV - cont...(13:00-16:59 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - Physical Security - Bypassing Access Control Systems - Andrew Johnson
RTV - Level UP OSINT - Mishaal Khan
RTV - Modifying Impacket for Better OpSec - Ryan O'Donnell
RTV - cont...(13:00-14:50 PDT) - Badge Cloning: A Penetration Tester's Guide to Capturing and Writing Badges - Travis

Weathers,Ralph May
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - Election 2024 Freedom of Choice: A Psybernomic Conundrum - Hallie Stern,Tina Schneibs
VMV - (14:30-14:45 PDT) - Risk Limiting Audit DEMO by Philip Stark - Philip Stark
VMV - (14:45-15:30 PDT) - What Does it Mean to be an American? - Kendall Spencer
WS - Sold Out - Ghidra Analysis & Automation Masterclass - Max "Libra" Kersten
WS - Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF - Alek Amrani,Ryan Holeman
WS - Sold Out - Hack the connected plant! - Alexandrine Torrents,Arnaud Soullié
WS - Sold Out - From an attacker's lair to your home: A practical journey through the world of Malware - Sebastian Tapia De la torre
WS - Sold Out - Dissecting and Defeating Ransomware's Evasion Tactics - Aaron Rosenmund,Josh Stroschein,Ryan Chapman
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - Extend reality with tabletop RPG OWASP Cornucopia. Play sessions throughout workshop times. - Stryker

Friday - 15:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - Hands-on workshop -
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - On Your Ocean's 11 Team, I'm the AI Guy (technically Girl) - Harriet Farlow
AIxCC - Closing the Software Vulnerability Gap - Dr. Kathleen Fisher
APV - Arsenal: HunterBounter - Swiss Army Knife for Bug Bounty - Utku Yildirim
APV - Arsenal: Introducing RAVEN - Discovering and Analyzing CI/CD Vulnerabilities in Scale - Elad Pticha,Oreen Livni
APV - The Open Source Fortress: Finding Vulnerabilities in Your Codebase Using Open Source Tools - iosifache
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - cont...(14:45-15:15 PDT) - Threat Modeling in the Age of AI - Adam Shostack
APV - (15:30-15:59 PDT) - Fine Grained Authorisation with Relationship-Based Access Control - Ben Dechrai
APV - Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - mcdwayne
APV - Activity: Hacking Developers' Trust – Faking GitHub Contribution by Checkmarx - Tal Folkman,Ori Ron,Mário Leitão-Teixeira
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - (15:30-17:30 PDT) - Space Pirate Simulator - Michael Butler,Jacob Oakley
ASV - (15:30-15:59 PDT) - Ground Control to Major Threat - Hacking the Space Link Extension Protocol - Andrzej Olchawa
BBV - Prototype Pollution in Depth, From Beginner to 0-Day Hunter - Lucas Philippe
BHV - Breaking Boundaries: Popping Shells in the Airgap with $10 and a Dash of Arduino Magic - Daniel Beard
BHV - (15:30-15:59 PDT) - Dysfunctional Unity: The Road to Nowhere - Michael "v3ga" Aguilar
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - Life, Liberty and the pursuit of Convenience: the slow death of independence - Kaleeque Pierce
BTV - cont...(14:00-15:59 PDT) - Area DC32: An Interactive Tabletop Takes Flight (A BTV Panel) - Aakin Patel,Caspian Kilkelly,Gwyddia,Harlan Geer,Shea Nangle,Matt Mayes
BTV - cont...(14:30-15:30 PDT) - BTV Conversations: Exploring the Cyberpsychology of Cyber Defender Acceptance Behaviors and Personality Traits - Todd Fletcher
BTV - (15:30-16:30 PDT) - BTV Conversations: Touch Grass to Combat Burnout - CtrlAltFu
CHV - Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack - Kevin Mitchell
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(14:30-15:10 PDT) - Attacking and Defending Software Supply Chains: How we got Admin in your Clouds! - Mike Ruth

CLV - Epyon - Attacking DevOps environments - Victor Pasknel
CLV - (15:40-17:40 PDT) - Hands-On Container Image Security: Mastering Sigstore for Unbreachable Integrity - Mohammed Ilyas Ahmed,Syed Aamiruddin
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(14:00-15:59 PDT) - Hack3r Runw@y - Signups -
CON - cont...(10:00-16:30 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-15:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC’s Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(12:00-19:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-17:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(12:00-16:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(09:00-16:59 PDT) - Social Engineering Community Vishing Competition (SECVC) -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -

CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CPV - Basic Mobile Phone Privacy - Grey Fox
DC - DC101 Panel - Nikita Kronenberg,Drew "aNullValue" Stemen,Grifter,AdaZebra
DC - Abusing Windows Hello Without a Severed Hand - Ceri Coburn,Dirk-jan Mollema
DC - cont...(14:30-15:15 PDT) - Breaching AWS Accounts Through Shadow Resources - Yakir Kadkoda,Michael Katchinskiy,Ofek Itach
DC - (15:30-16:15 PDT) - Taming the Beast: Inside the Llama 3 Red Team Process - Aaron "dyn" Grattafiori,Ivan Evtimov,Joanna Bitton,Maya Pavlova
DC - Android App Usage and Cell Tower Location: Private. Sensitive. Available to Anyone? - Ryan Johnson
DC - cont...(14:30-15:15 PDT) - Joe and Bruno's Guide to Hacking Time: Regenerating Passwords from RoboForm's Password Generator - Joe "Kingpin" Grand,Bruno Krauss
DC - (15:30-16:15 PDT) - Social Engineering Like you're Picard - Jayson E. Street
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - cont...(14:00-15:45 PDT) - Automated Control Validation with Tommyknocker - Jeremy Banker
DL - cont...(14:00-15:45 PDT) - HIDe & SEEK - Jonathan Fischer,Matthew Richard
DL - cont...(14:00-15:45 PDT) - SCAGoat - Exploiting Damn Vulnerable SCA Application - Hare Krishna Rai,Prashant Venkatesh
DL - cont...(14:00-15:45 PDT) - Garak - Erick Galinkin,Leon Derczynski
DL - cont...(14:00-15:45 PDT) - XenoboxX - Hardware Sandbox Toolkit - Cesare Pizzi
DL - cont...(14:00-15:45 PDT) - Hopper - Distributed Fuzzer - Luciano Remes,Wade Cappa
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(14:00-15:59 PDT) - HDA Presents : Naomi Brockwell - Naomi Brockwell
HRV - cont...(13:00-15:59 PDT) - Ham Radio Exams -
ICSV - The People's Republic of Fieldbus: What to know about EPA - Jonathan Reiter
ICSV - (15:30-15:55 PDT) - OT Incident response and Threat Hunting - Adam Robbie,Bradley Nash
IOTV - cont...(14:30-15:30 PDT) - Exploration of Cellular Based IoT Technology - Carlota Bindner,Deral Heiland
IOTV - (15:30-15:59 PDT) - Microhard? More like MicroEASY...to exploit... - Ricky "HeadlessZeke" Lawshae
IOTV - (15:50-16:30 PDT) - Where's the Money: Defeating ATM Disk Encryption - Matt Burch
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(14:00-15:59 PDT) - Solder your own cat shaped WiFi Haking tool - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
LPV - cont...(13:00-15:59 PDT) - Safecracking Practical Demonstration - Jared Dygert

MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(14:00-15:59 PDT) - Friendship Bracelet Making -
MISC - C2Society / DC702 Intro to CTFs -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(11:30-17:30 PDT) - Book Signings -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(14:00-17:59 PDT) - Resume Reviews -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Generative AI vs Crusty NCO - Col Travis Hartman
MISC - Removing OPSEC from Cyber Predators and Threat Actors - Thiago Bordini
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PLV - cont...(14:30-15:15 PDT) - Human Dignity in AI and Tech Policy - Jan Trzaskowski
PLV - (15:15-15:59 PDT) - Open Source Hacker Vs. Government Lawyer: Clashing Views on Fixing Tech in the DoD - Eddie Zaneski,Rebecca Lively
PLV - NSM-22 and the National Risk Management Plan: CISA Wants to Hear from You on How to Protect Our Nation’s Critical Infrastructure - William Loomis,Michael Garcia
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - cont...(14:30-15:30 PDT) - Your Smartcard is Dumb: A Brief History of Hacking Access Control Systems - Chad Shortman
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - cont...(14:30-15:10 PDT) - Emulating Magstripe with Arduino - Leigh-Anne Galloway
QTV - Trapped Ion Quantum Computing Systems - Behind The Scenes: from the physics to control electronics - Daiwei Zhu,Rick Altherr
RCV - cont...(14:00-17:59 PDT) - ToolMakers Hackathon -
RCV - Interview - Scott Helme, Hosted by Shubham - Scott Helme,Shubham
RCV - GeoINT Mastery: A pixel is worth a thousand words - Mishaal Khan
RCV - (15:45-16:20 PDT) - Recon MindMap: Organize, Visualize, and Prioritize Your Recon Data Efficiently - Lenin Alevski
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(14:30-15:25 PDT) - Yet another way of exfiltrating data from air-gapped systems OR Oh no, everything is a radio - C$,Endeavors

RFV - (15:30-15:55 PDT) - Warwheeling: The Wireless Sk8r - r1otctrl
RTV - cont...(13:00-16:59 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - Threat Emulation 101 - Trey Bilbrey
RTV - New Skill Unlocked: C2 Infrastructure Automation - Josh Huff,Robert Pimentel
RTV - cont...(14:00-15:50 PDT) - Modifying Impacket for Better OpSec - Ryan O'Donnell
RTV - GHOST in the Model: Generating AI-Assisted Threat Models for Efficient Offensive Security Testing - Sam Cosentino
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
TCV - Telecom Time Machine - Nadeem Bagwan
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - cont...(14:45-15:30 PDT) - What Does it Mean to be an American? - Kendall Spencer
VMV - (15:30-16:15 PDT) - Breaking Through Election Myths - Will Baggett
WS - cont...(14:00-17:59 PDT) - Sold Out - Ghidra Analysis & Automation Masterclass - Max "Libra" Kersten
WS - cont...(14:00-17:59 PDT) - Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF - Alek Amrani,Ryan Holeman
WS - cont...(14:00-17:59 PDT) - Sold Out - Hack the connected plant! - Alexandrine Torrents,Arnaud Soullié
WS - cont...(14:00-17:59 PDT) - Sold Out - From an attacker's lair to your home: A practical journey through the world of Malware - Sebastian Tapia De la torre
WS - cont...(14:00-17:59 PDT) - Sold Out - Dissecting and Defeating Ransomware's Evasion Tactics - Aaron Rosenmund,Josh Stroschein,Ryan Chapman
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(14:00-17:59 PDT) - Extend reality with tabletop RPG OWASP Cornucopia. Play sessions throughout workshop times. - Stryker

Friday - 16:00 PDT

Return to Index - Locations Legend

ADV - (16:30-16:59 PDT) - Master Splinter's initial physical access dojo: Storytelling of a complex adversarial attack - Daniel Isler
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(15:00-16:59 PDT) - Hands-on workshop -
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - AI Village Day 1 Keynote – Poison, injection, evasion, oh my! Grounding AI security threats in data driven reality - Christina Liaghati
AIxCC - Industry Panel: The Modern Evolution of LLMs - Dr. Matt Turek,Heather Adkins,Jason Clinton,Matt Knight,David Weston
AIxCC - (16:55-17:15 PDT) - No Time for Complacency: The Stakes of AI in Cybersecurity - Heather Adkins
APV - cont...(15:00-17:30 PDT) - The Open Source Fortress: Finding Vulnerabilities in Your Codebase Using Open Source Tools - iosifache
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - (16:15-16:45 PDT) - I've got 99 problems but a prompt injection ain't watermelon - Chloé Messdaghi,Kasimir Schulz
APV - cont...(15:00-16:59 PDT) - Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - mcdwayne
APV - cont...(15:00-16:59 PDT) - Activity: Hacking Developers' Trust – Faking GitHub Contribution by Checkmarx - Tal Folkman,Ori Ron,Mário Leitão-Teixeira
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(15:30-17:30 PDT) - Space Pirate Simulator - Michael Butler,Jacob Oakley
ASV - Analyzing the Security of Satellite-Based Air Traffic Control - Martin Strohmeier
BBV - cont...(15:00-16:30 PDT) - Prototype Pollution in Depth, From Beginner to 0-Day Hunter - Lucas Philippe
BBV - (16:30-17:59 PDT) - LFG! Forming a Bug Bounty Hunting Party - Harrison Richardson
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - The Implications of Cyberbiosecurity in Advanced Agricultural Systems - Simone Stephen
BTV - cont...(15:30-16:30 PDT) - BTV Conversations: Touch Grass to Combat Burnout - CtrlAltFu
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(15:40-17:40 PDT) - Hands-On Container Image Security: Mastering Sigstore for Unbreachable Integrity - Mohammed Ilyas Ahmed,Syed Aamiruddin
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -

CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-16:30 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(12:00-19:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-17:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(12:00-16:59 PDT) - Red Alert ICS CTF -
CON - Pub Quiz -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(09:00-16:59 PDT) - Social Engineering Community Vishing Competition (SECVC) -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-16:59 PDT) - Blacks in Cyber CTF -
CPV - Data On Demand: The challenges of building a privacy focused AI Device - Matt Domko
DC - Making the DEF CON 32 Badge - Mar Williams

DC - Eradicating Hepatitis C With BioTerrorism - Mixæl Swan Laufer
DC - cont...(15:30-16:15 PDT) - Taming the Beast: Inside the Llama 3 Red Team Process - Aaron "dyn" Grattafiori,Ivan Evtimov,Joanna Bitton,Maya Pavlova
DC - (16:30-17:15 PDT) - Leveraging private APNs for mobile network traffic analysis - Aapo Oksman
DC - Outlook Unleashing RCE Chaos: CVE-2024-30103 & CVE-2024-38021 - Michael Gorelik ,Arnold Osipov
DC - cont...(15:30-16:15 PDT) - Social Engineering Like you're Picard - Jayson E. Street
DC - (16:30-17:15 PDT) - Why are you still, using my server for your internet access. - Thomas Boejstrup Johansen
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
ICSV - Correlating & contextualizing OT events/alerts/logs using weakly supervised AI - Ezz Tahoun
ICSV - (16:30-16:59 PDT) - ICS 101 - Bryson Bort ,Tom VanNorman
IOTV - cont...(15:50-16:30 PDT) - Where's the Money: Defeating ATM Disk Encryption - Matt Burch
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - (16:30-17:59 PDT) - Meshtastic Meetup - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - (16:30-17:30 PDT) - So you wanna know how to make badges - c0ldbru
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(15:00-17:59 PDT) - C2Society / DC702 Intro to CTFs -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(11:30-17:30 PDT) - Book Signings -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(14:00-17:59 PDT) - Resume Reviews -
MISC - Name the Noob -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -

MISC - Structural Insights: PDF Analysis for Detecting and Defending Against Threats - Filipi Pires
MISC - (16:30-16:59 PDT) - Chatbots for Cybersecurity - Lenin Alevski
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PLV - Cybersecurity Schoolhouse Rock - Avi McGrady
PLV - cont...(15:00-16:45 PDT) - NSM-22 and the National Risk Management Plan: CISA Wants to Hear from You on How to Protect Our Nation's Critical Infrastructure - William Loomis,Michael Garcia
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - Access Control done right the first time - Tim Clevenger
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - (16:30-16:59 PDT) - Payment Village CTF Day One Results -
QTV - Attack Vectors of Quantum Computers - Sorin Boloș,Adrian Coleșa
RCV - cont...(14:00-17:59 PDT) - ToolMakers Hackathon -
RCV - cont...(15:45-16:20 PDT) - Recon MindMap: Organize, Visualize, and Prioritize Your Recon Data Efficiently - Lenin Alevski
RCV - Interview - the gumshoo, Hosted by Ram - the gumshoo,Ram
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - A Short Introduction to 802.11ah Long Range WiFi HaLow with TaiXin TXW8301 devices - Ronald Broberg,Robert Van Etta
RFV - (16:30-17:25 PDT) - Meshtastic Adventures: Triumphs, Tribulations, and Total Mesh-ups. - m1ddl3w4r3
RTV - cont...(13:00-16:59 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - Mac-n-Cheese: How to Cook Up Delicious Electron Techniques for Red Teamers - Roberto Soares
RTV - cont...(15:00-16:50 PDT) - New Skill Unlocked: C2 Infrastructure Automation - Josh Huff,Robert Pimentel
RTV - Thinking Outside the Kube - Finding and Exploiting Command Injections in Kubernetes - Tomer Peled
RTV - Building Your Red-Teaming Co-Pilot: Navigating the New Cyber Era with Pretrained Gen-AI - Gaspard Baye
RTV - Blue Goes Purple: Purple Teams for Fun and Profit (A BTV & RTV Panel) - Catherine J. Ullman,Jake Williams,Meaghan Neill,Ralph May,Matthew Nickerson
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
SOC - DEF CON Holland Group Presents: VrijMiBo -
SOC - QueerCon Mixer -
SOC - DCG Atlanta (DC404,678,770,470) -
TCV - cont...(15:00-16:59 PDT) - Telecom Time Machine - Nadeem Bagwan
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - cont...(15:30-16:15 PDT) - Breaking Through Election Myths - Will Baggett
VMV - (16:15-16:59 PDT) - Maricopa County -Preparing for the 2024 Elections Cycle - Nate Young,Jason Butryn
WS - cont...(14:00-17:59 PDT) - Sold Out - Ghidra Analysis & Automation Masterclass - Max "Libra" Kersten
WS - cont...(14:00-17:59 PDT) - Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF - Alek Amrani,Ryan Holeman
WS - cont...(14:00-17:59 PDT) - Sold Out - Hack the connected plant! - Alexandrine Torrents,Arnaud Soullié
WS - cont...(14:00-17:59 PDT) - Sold Out - From an attacker's lair to your home: A practical journey through the world of Malware - Sebastian Tapia De la torre
WS - cont...(14:00-17:59 PDT) - Sold Out - Dissecting and Defeating Ransomware's Evasion Tactics - Aaron Rosenmund,Josh Stroschein,Ryan Chapman
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(14:00-17:59 PDT) - Extend reality with tabletop RPG OWASP Cornucopia. Play sessions throughout workshop times. - Stryker

Friday - 17:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - Red Teaming is broken; this panel will fix it. - Suneel Sundar,Niru Ragupathy,Joe Vest,Drinor Selmanaj
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIxCC - cont...(16:55-17:15 PDT) - No Time for Complacency: The Stakes of AI in Cybersecurity - Heather Adkins
AIxCC - (17:20-17:59 PDT) - How Competitions Can Fuel Innovation - Mike Walker,Matt Knight,Ruoyu "Fish" Wang
APV - cont...(15:00-17:30 PDT) - The Open Source Fortress: Finding Vulnerabilities in Your Codebase Using Open Source Tools - iosifache
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - When Chatbots Go Rogue – Lessons Learned from Building and Defending LLM Applications - Andra,Javan Rasokat
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(15:30-17:30 PDT) - Space Pirate Simulator - Michael Butler,Jacob Oakley
BBV - cont...(16:30-17:59 PDT) - LFG! Forming a Bug Bounty Hunting Party - Harrison Richardson
BBV - Reflections on a Decade in Bug Bounties: Experiences and Major Takeaways - Charles Waterhouse,Nikhil "niks" Shrivastava
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BTV - CTI is Dead, Long Live CTI: Reassessing Blue Team's Squishiest Value Proposition (BTV Panel) - Aurora Johnson,Ben Goerz,Ch33r10,Jamie Williams,Rebecca Ford
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(15:40-17:40 PDT) - Hands-On Container Image Security: Mastering Sigstore for Unbreachable Integrity - Mohammed Ilyas Ahmed,Syed Aamiruddin
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -

CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(12:00-19:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:30-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-17:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(16:00-18:59 PDT) - Pub Quiz -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cyber CTF -
CON - cont...(09:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
CPV - (17:30-17:59 PDT) - Fool us Once, fool us twice... Hacking Norwegian Banks - Cecilie Wian,Per Thorsheim
DC - Bricked & Abandoned: How To Keep The IoT From Becoming An Internet of Trash - Paul Roberts,Chris Wysopal,Cory Doctorow,Tarah Wheeler,Dennis Giese
DC - One for all and all for WHAD: wireless shenanigans made easy ! - Damien Cauquil,Romain Cayre
DC - cont...(16:30-17:15 PDT) - Leveraging private APNs for mobile network traffic analysis - Aapo Oksman
DC - (17:30-18:15 PDT) - Exploiting Bluetooth - from your car to the bank account$$ - Vladyslav Zubkov,Martin Strohmeier
DC - Breaking Secure Web Gateways (SWG) for Fun and Profit - Vivek Ramachandran,Jeswin Mathai
DC - cont...(16:30-17:15 PDT) - Why are you still, using my server for your internet access. - Thomas Boejstrup Johansen
DC - (17:30-17:50 PDT) - Stranger in a Changed Land - Tony Sager
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -

IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(16:30-17:59 PDT) - Meshtastic Meetup - Kody K
IOTV - Beyond Sunset: Exposing the Occultations Lurking in Large-Scale Off-Grid Solar Systems - Alexandru Lazar,Dan Berte
IOTV - (17:30-17:59 PDT) - Inside Dash Cam: Custom Protocols and Discovered 0-days - Hyo Jin Lee,Hanryeol Park
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(16:30-17:30 PDT) - So you wanna know how to make badges - c0ldbru
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(15:00-17:59 PDT) - C2Society / DC702 Intro to CTFs -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(11:30-17:30 PDT) - Book Signings -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(14:00-17:59 PDT) - Resume Reviews -
MISC - cont...(16:00-17:59 PDT) - Name the Noob -
MISC - cont...(08:00-17:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Cybersecurity Overview over LATAM- Skills, Challenges, Knowledge, Perspectives - Leonardo Pigñer,Katherina Canales,Victor Santos
MISC - (17:30-21:30 PDT) - Ask the EFF -
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PLV - Singapore - Safeguarding the Nation: The Vital Role of Cybersecurity in AI-Driven Homeland Security - NG Yeow Boon,Bill Woodcock
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - Bypass 101 - Karen Ng

QTV - DevSecOps of Quantum Computers -
QTV - (17:30-17:59 PDT) - Threat Modelling: Quantum Computers -
RCV - cont...(14:00-17:59 PDT) - ToolMakers Hackathon -
RCV - Pushing the limits of mass DNS scanning - Jasper Insinger
RCV - (17:45-18:15 PDT) - OSINT at Clemson: Unmasking John Mark Dougan's Disinformation Empire - Steven Sheffield
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(16:30-17:25 PDT) - Meshtastic Adventures: Triumphs, Tribulations, and Total Mesh-ups. - m1ddl3w4r3
SEV - cont...(08:30-17:59 PDT) - Social Engineering Community Village Hours -
SEV - (17:15-17:59 PDT) - Presentation: The 2024 #SECVC Debrief -
SOC - cont...(16:00-18:59 PDT) - DEF CON Holland Group Presents: VrijMiBo -
SOC - cont...(16:00-17:59 PDT) - QueerCon Mixer -
SOC - cont...(16:00-18:59 PDT) - DCG Atlanta (DC404,678,770,470) -
SOC - Friends of Bill W -
TCV - SIMply Secure - Zibran Sayyed
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - Hacking the Vote: How Hackers Caused the Downfall of the Dutch Voting Machines - Fleur van Leusden
WS - cont...(14:00-17:59 PDT) - Sold Out - Ghidra Analysis & Automation Masterclass - Max "Libra" Kersten
WS - cont...(14:00-17:59 PDT) - Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF - Alek Amrani,Ryan Holeman
WS - cont...(14:00-17:59 PDT) - Sold Out - Hack the connected plant! - Alexandrine Torrents,Arnaud Soullié
WS - cont...(14:00-17:59 PDT) - Sold Out - From an attacker's lair to your home: A practical journey through the world of Malware - Sebastian Tapia De la torre
WS - cont...(14:00-17:59 PDT) - Sold Out - Dissecting and Defeating Ransomware's Evasion Tactics - Aaron Rosenmund,Josh Stroschein,Ryan Chapman
XRV - Be the Ghost in the Shell Barrier Mazes FTW - David "Icer" Maynor
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(14:00-17:59 PDT) - Extend reality with tabletop RPG OWASP Cornucopia. Play sessions throughout workshop times. - Stryker

Friday - 18:00 PDT

Return to Index - Locations Legend

CON - (18:30-19:30 PDT) - Whose Slide Is It Anyway? -
CON - cont...(12:00-19:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(16:00-18:59 PDT) - Pub Quiz -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
DC - cont...(17:30-18:15 PDT) - Exploiting Bluetooth - from your car to the bank account$$ - Vladyslav Zubkov,Martin Strohmeier
DC - DEF CON Franklin Project - Jacob H Braun
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - HDA Chillout w/ Dj Delchi -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(17:30-21:30 PDT) - Ask the EFF -
RCV - cont...(17:45-18:15 PDT) - OSINT at Clemson: Unmasking John Mark Dougan's Disinformation Empire - Steven Sheffield
SOC - cont...(16:00-18:59 PDT) - DEF CON Holland Group Presents: VrijMiBo -
SOC - cont...(16:00-18:59 PDT) - DCG Atlanta (DC404,678,770,470) -
SOC - (18:30-22:30 PDT) - Policy Mixer @ DEF CON -

Friday - 19:00 PDT

Return to Index - Locations Legend

CON - cont...(18:30-19:30 PDT) - Whose Slide Is It Anyway? -
CON - cont...(12:00-19:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(18:00-23:59 PDT) - HDA Chillout w/ Dj Delchi -
MISC - cont...(08:00-19:59 PDT) - Human Registration Open -
MISC - cont...(17:30-21:30 PDT) - Ask the EFF -
SOC - (19:30-21:59 PDT) - Lawyers Meet -
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -
SOC - BlanketFort Con -
SOC - Blacks in Cyber Lituation 2.0 - BIC Village Staff,DJ Roma

Friday - 20:00 PDT

Return to Index - Locations Legend

CON - Hacker Jeopardy -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(18:00-23:59 PDT) - HDA Chillout w/ Dj Delchi -
MISC - cont...(17:30-21:30 PDT) - Ask the EFF -
MISC - DEF CON Movie Night -
SOC - Music Set / Entertainment (Cyberpunk Bar Friday, ACK Stage) - Scotch & Bubbles,PankleDank,DJ St3rling,DJ Habbs,Call the Cops,Archwisp
SOC - Hacker Karaoke -
SOC - cont...(19:30-21:59 PDT) - Lawyers Meet -
SOC - Music Set / Entertainment (Retro Sci-Fi Friday, SYN Stage) - ZEE,YTCracker,TRIODE,Ohm-I & The NPC Collective,MC Frontalot,Icetre Normal,Dual Core,Costume Contest
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -

Friday - 21:00 PDT

Return to Index - Locations Legend

CON - cont...(20:00-21:59 PDT) - Hacker Jeopardy -
CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(18:00-23:59 PDT) - HDA Chillout w/ Dj Delchi -
MISC - Capitol Technology University (CTU) -
MISC - cont...(17:30-21:30 PDT) - Ask the EFF -
MISC - cont...(20:00-23:59 PDT) - DEF CON Movie Night -
SOC - Arcade Party -
SOC - cont...(19:30-21:59 PDT) - Lawyers Meet -
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -
SOC - GOTHCON 2024 -

Friday - 22:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(18:00-23:59 PDT) - HDA Chillout w/ Dj Delchi -
MISC - cont...(20:00-23:59 PDT) - DEF CON Movie Night -
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -
SOC - QueerCon -

Friday - 23:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-23:59 PDT) - Cloud Village CTF -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(18:00-23:59 PDT) - HDA Chillout w/ Dj Delchi -
MISC - cont...(20:00-23:59 PDT) - DEF CON Movie Night -

Saturday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Saturday - 05:00 PDT

Return to Index - Locations Legend

MISC - Defcon.run -

Saturday - 06:00 PDT

Return to Index - Locations Legend

MISC - cont...(05:00-07:59 PDT) - Defcon.run -

Saturday - 07:00 PDT

Return to Index - Locations Legend

MISC - cont...(05:00-07:59 PDT) - Defcon.run -

Saturday - 08:00 PDT

Return to Index - Locations Legend

MISC - Human Registration Open -
MISC - Lost & Found -

Saturday - 09:00 PDT

Return to Index - Locations Legend

MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - Merch (formerly swag) Area Open -- README -
WS - Sold Out - Sharp Security from All Angles: Mastering Security in .NET Core 8 and Angular 17 Applications - Or Sahar,Yariv Tal
WS - Sold Out - Hacking The Metal: A Spark of Intelligence - eigentourist
WS - Sold Out - Capture the Flag 101 - Micah Silverman
WS - Sold Out - Hacking Apps on Salesforce - Rodney David Beede
WS - Sold Out - Industrial Control Systems: how to secure them in practice! - Alexandrine Torrents

Saturday - 10:00 PDT

Return to Index - Locations Legend

ADV - Sneaky Extensions: The MV3 Escape Artists - Vivek Ramachandran,Shourya Pratap Singh
ADV - (10:30-10:59 PDT) - Tough Adversary? Don't Blame Sun Tzu - Gregory Carpenter
ADV - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - Adversarial AI: Disrupting Artificial Intelligence with Style - Chloé Messdaghi,Sebastian Cesario,Kasimir Schulz
AIV - AI Village Demos -
AIV - Keynote - AI-Powered Cybersecurity: The Importance of Red Teamers - Nikki Pope
AIxCC - Securing Health Care: AIxCC, DIGIHEALS, and UPGRADE - Dr. Jennifer Roberts,Dr. Susan Coller Monarez,Andrew Carney
APV - Fix the Flag Wargame - Harley Wilson
APV - (10:15-10:55 PDT) - Navigating the Cyber Security Labyrinth: Choose Your Own Security Adventure? - punkcoder
ASV - Space Systems Security CTF – Platform Security - CT Cubed
ASV - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - ARINC 664 CTF - Boeing
ASV - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - Space Grand Challenge Luna - CalPoly
ASV - Selfie with a CubeSat - CalPoly
ASV - PTP Flight Challenge - Pen Test Partners
ASV - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - Drone Capture the Flag (CTF) - Dark Wolf
ASV - Drone Flying Experience - Dark Wolf
ASV - Drone Hacking Activity - Dark Wolf
ASV - Detect a Threat - TSA
ASV - Bricks in the Air -
ASV - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - Darkstar Badge Challenge - Lockheed Martin
ASV - CubeSat Simulator - AMSAT
ASV - (10:30-11:30 PDT) - Introduction to Drone Security - Hahna Kane Latonick
BBV - Leveraging Internal Systems for Enhanced Bug Bounty Success - Rotem Bar
BHV - Bridging Space and Medicine - Fernando De La Peña Llaca
BHV - Biohacking Village: Device Lab -
BICV - Fumbling into FedCyber - Nikkia Henderson
BICV - (10:45-11:30 PDT) - Unmasking Shadows: Strategies on Hunting Ransomware Groups - R.J. McCarley
BTV - Securing the Cloud with Cloud Threat Intelligence and Open Source Security - Natalie Simpson,Nivedita (Nivu) Jejurikar
BTV - Obsidian: Forensics 101 Part 1 - Sarthak Taneja
BTV - (10:30-10:59 PDT) - Obsidian: Forensics 101 Part 2 - Sarthak Taneja
CHV - Car Hacking Village Activities -
CLV - GCPwn: A Pentester's GCP Tool - Scott Weston
CLV - (10:30-11:10 PDT) - Terraform Unleashed: Crafting Custom Provider Exploits for Ultimate Control - Alex Foley,Rupali
CON - IoT Village CTF -
CON - Cloud Village CTF -
CON - Hardware Hacking Village CTF -
CON - Radio Frequency Capture the Flag -
CON - Embedded CTF -
CON - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - Biohacking Village CTF -

CON - QOLOSSUS -
CON - ICS CTF -
CON - Car Hacking Village CTF -
CON - HackFortress -
CON - Tinfoil Hat Contest -
CON - Chasse Partie Systems CTF -
CON - CrackMeIfYouCan -
CON - DC's Next Top Threat Model (DCNTTM) -
CON - [CANCELED] AutoDriving CTF -
CON - Red Team Village CTF -
CON - Pinball High Score Contest -
CON - 5N4CK3Y Contest -
CON - Hac-Man -
CON - Darknet-NG -
CON - DC Kubernetes Capture the Flag (CTF) -
CON - ? Cube -
CON - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - PhreakMe presented by HackedExistence -
CON - REALI7Y OVERRUN -
CON - Lonely Tag -
CON - Lonely Hard Drive -
CON - A Wall of Bribes -
CON - spyVspy -
CON - DEF CON Scavenger Hunt -
CON - Malware Contests: MARC I & BOMBE -
CON - Live Recon Contest in Progress -
CON - Adversary Wars CTF -
CON - HTB CTF: Data Dystopia -
CON - Octopus Game -
CON - Cyber Defender - The Game -
CON - CMD+CTRL at DEF CON 32 -
CON - Red Alert ICS CTF -
CON - HardWired -
CON - Capture the Packet -
CON - (10:30-17:59 PDT) - Blue Team Village CTF -
CON - Blacks in Cyber CTF -
CON - Blacks in Cyber CTF -
CON - Social Engineering Community Youth Challenge -
CON - It's In That Place Where I Put That Thing That Time -
CON - venator aurum - A Treasure Hunt -
CPV - (10:25-10:30 PDT) - CPV: Day 2 Welcome -
CPV - (10:30-10:45 PDT) - CPV: Intro to Cyphers -
DC - The Pwnie Awards -
DC - Laundering Money - Michael Orlitzky
DC - (10:30-11:15 PDT) - Gotta Cache 'em all: bending the rules of web cache exploitation - Martin Doyhenard
DC - Mutual authentication is optional - Xavier Zhang
DC - (10:30-11:15 PDT) - Smishing Smackdown: Unraveling the Threads of USPS Smishing and Fighting Back - S1nn3r
DC - Reverse Engineering MicroPython Frozen Modules: Data Structures, Reconstruction, and Reading Bytecode - Wesley McGrew
DC - CULT OF THE DEAD COW & Friends Present: Prime Cuts from Hacker History - 40 Years of 31337 - Deth Veggie,Walter J. Scheirer,Patrick "Lord Digital" Kroupa,John Threat,Emmanuel Goldstein,X,TommydCat
DCG - DEF CON Groups - Open for questions and hanging out -
DCGVR - Jayson Street - Keynote - Jayson E. Street
DCGVR - Jayson Street - Keynote - Jayson E. Street

DDV - DDV open and accepting drives for duplication -
DL - Maestro - Chris Thompson
DL - Tempest - Kirk Trychel
DL - 5Ghoul Framework - 5G NR Attacks & 5G OTA Fuzzing - Matheus Eduardo Garbelini,Sudipta Chattopadhyay
DL - Testbed Virtual Factory - Borja Pintos Castro,Camilo Piñón Blanco
DL - Cyber Security Transformation Chef (CSTC) - Florian Haag,Matthias Göhring
DL - MITRE Caldera - Mark Perry,Rachel Murphy
ESV - 101 Labs: Hardware Lab -
ESV - Hardware Hacking: Glitching Lab -
ESV - Secure Microcontroller Workshop -
ESV - Wireless & Networking workshop - Alex Kelly
ESV - 101 Labs: Firmware and Software exploitation -
ESV - Emulating (and Hacking) Embedded Devices -
HDA - HDA Community - Open for Accessibility Questions/Help -
ICSV - Securing the Harvest: Cyber Defense for Agricultural Control Systems - Ray Baeza
IOTV - SBOMs the Hard Way: Hacking Bob the Minion - Larry Pesce
IOTV - (10:30-11:15 PDT) - Psychic Paper: Making eink access badges accessible for anyone - Joshua Herman
IOTV - Safe Hacking -
IOTV - Keysight CTF Challenge -
IOTV - IoT Village Hacking Playground -
IOTV - Phisherman's Wharf - Phishing for Beginners -
IOTV - IoT Security at DEF CON 32 -
IOTV - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - Firmware Extraction and Analysis -
IOTV - Hack My TV -
IOTV - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - Hardware Hacking GE Appliances -
IOTV - (10:15-11:45 PDT) - Learn BadUSB Hacking With the USB Nugget - Kody K
LPV - Lockpicking Activities -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - Vendors and Exhibitors Open -
MISC - All content areas generally open -
MISC - Hard Hat Brigade - Community Space Open -
MISC - Robo Sumo -
MISC - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - HHV Rube Goldberg Machine -
MISC - WISP Community & Inclusion Room -
MISC - Intro to Circuit Python (Badge class level 1) (Overflow if Friday is too full) -
MISC - Game Hacking Community Activities & CTF -
MISC - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - Small scale LAN party -
MISC - Retro Repair -
MISC - Dumb Terminal fun -
MISC - Show & Tell -
MISC - Egor's Keyboard Corner -
MISC - LHC's Unofficial Sticker Swap Table -
MISC - Resume Reviews -
MISC - Lonely Hackers Club Community Room Open -
MISC - LHC Meshtastic Activities and CTF -
MISC - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Case Study: Hacking Smart Lock For Fun and Profit - Cesar Ortega Ortega
MISC - (10:30-11:30 PDT) - Protecting the Backbone of Our Modern World - Soledad Antelada Toledano

MISC - Open Events for DCNextGen -
PHV - Packet Inspector -
PHV - Regular Expressions (RegEx) Trainer -
PHV - Network-OS: Be The Cloud -
PHV - Packet Detective -
PHV - Botnets -
PHV - Linux Trainer -
PHV - Python + Packet Analysis + Machine Learning -
PHV - Password lab -
PHV - FleetDm -
PHV - Using AI Computer Vision in Your OSINT Data Analysis - Mike Raggo
PSV - Physical Security Village Activities -
PYV - Payment Village CTF -
PYV - (10:15-10:20 PDT) - Introduction to Payment Village CTF - Leigh-Anne Galloway
PYV - (10:45-10:59 PDT) - Introduction to the Payment Village badge - Leigh-Anne Galloway
QTV - Intro to QKD: Quantum Key Exchange: Beyond the Hype - Ben Varcoe
RCV - Maltego Community Workshop - Carlos Fragoso
RCV - Recon Village GE(O)SINT Challenge -
RCV - Interview - CATO Networks, Hosted by Dhruv Shah - CATO Networks,Dhruv Shah
RFV - Radio Frequency Village Events -
RFV - (10:30-11:25 PDT) - RF CTF Kick Off Day 2 - RF Hackers
RTV - The Hybrid Horizon: Unleashing the Power of Azure Hybrid Integrations - Chirag Savla,Raunak Parmar
RTV - BOAZ, Yet Another layered Evasion Tool: Unveiling the Secrets Behind Antivirus Testing - Thomas X Meng
RTV - DoH Deception: Evading ML-Based Tunnel Detection with Black-Box Attack Techniques - Emanuel Valente
RTV - Physical Red Teaming for Offensive Cyber Teams - Shawn Abelson,Ana Aslanishvili
RTV - Hacking the Skies – Satellite Red Teaming - Agostino Panico
SEV - John Henry Competition - Human vs. AI & Panel Discussion -
SEV - Social Engineering Community Village Hours -
TCV - AI-Driven Cyber Resilience: Surviving the 5G Threat Landscape - Shina Liu,Niklas Lindroos,Ezz Tahoun,Akib Sayyed
TEV - Tamper Evident Village Activities -
VMV - Voting Village Opening Remarks - Catherine Terranova,Harri Hursti,Matt Blaze
WS - cont...(09:00-12:59 PDT) - Sold Out - Sharp Security from All Angles: Mastering Security in .NET Core 8 and Angular 17 Applications - Or Sahar,Yariv Tal
WS - cont...(09:00-12:59 PDT) - Sold Out - Hacking The Metal: A Spark of Intelligence - eigentourist
WS - cont...(09:00-12:59 PDT) - Sold Out - Capture the Flag 101 - Micah Silverman
WS - cont...(09:00-12:59 PDT) - Sold Out - Hacking Apps on Salesforce - Rodney David Beede
WS - cont...(09:00-12:59 PDT) - Sold Out - Industrial Control Systems: how to secure them in practice! - Alexandrine Torrents
XRV - ICS Village + XR Village Turn the lights on! -
XRV - Signals Are Everywhere -

Saturday - 11:00 PDT

Return to Index - Locations Legend

ADV - Evading Modern Defenses When Phishing with Pixels - Melvin Langvik
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - Power To The Purple - Tyler Casey,Trey Bilbrey
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - (11:30-12:30 PDT) - garak : A Framework for Large Language Model Red Teaming - Leon Derczynski,Erick Galinkin,Jeffery Martin,Subho Majumdar
AIxCC - (11:30-11:50 PDT) - Spotting Deepfakes in a World with Generative AI - Dr. William Corvey
APV - Arsenal: SCAGoat - Gaurav Joshi,HK,kvprashant
APV - Application Threat Modeling with Trike - AreTillery
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - BOLABuster: Harnessing LLMs for Automating BOLA Detection - Jay Chen,Ravid Mazon
APV - (11:40-12:10 PDT) - Unlocking the Gates - Understanding Authentication Bypass Vulnerabilities - Vikas Khanna
APV - Activity: Vulnerability Hunt - The Snippets Edition - Mário Leitão-Teixeira
APV - Activity: API Security 101: Testing and Trivia by Akto.io - Ankush Jain,Ankita Gupta
APV - Activity: Capture the Container by Chainguard - Jonathan Leitschuh
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:30-11:30 PDT) - Introduction to Drone Security - Hahna Kane Latonick
BBV - The Bug Hunters Methodology Live - DEF CON Edition - Jason Haddix
BBV - (11:30-12:30 PDT) - Hunters and Gatherers: A Deep Dive into the World of Bug Bounties - Johnathan Kuskos,Katie Trimble-Noble,Sam (erbbysam) Erb,Jeff Guerra,Logan MacLaren
BHV - Eradicating Hepatitis C With BioTerrorism - Mixæl Swan Laufer
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - cont...(10:45-11:30 PDT) - Unmasking Shadows: Strategies on Hunting Ransomware Groups - R.J. McCarley
BICV - (11:30-12:15 PDT) - My Smart Red Team Copilot - Gaspard Baye
BTV - cont...(10:00-11:59 PDT) - Securing the Cloud with Cloud Threat Intelligence and Open Source Security - Natalie Simpson,Nivedita (Nivu) Jejurikar
BTV - (11:15-12:15 PDT) - Use opensource AI to map alerts & logs into techniques, clusters, and killchains - Ezz Tahoun
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(10:30-11:10 PDT) - Terraform Unleashed: Crafting Custom Provider Exploits for Ultimate Control - Alex Foley,Rupali
CLV - Identity Theft is not a Joke, Azure! - Karl Fosaaen

CLV - (11:50-12:15 PDT) - One Click, Six Services: Abusing The Dangerous Multi-service Orchestration Pattern - Liv Matan
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-16:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:00-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-15:59 PDT) - A Wall of Bribes -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-12:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(10:00-16:59 PDT) - Red Alert ICS CTF -
CON - DEF CON 32 Beard and Mustache Contest -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
DC - The Rise and Fall of Binary Exploitation - Stephen Sims
DC - cont...(10:30-11:15 PDT) - Gotta Cache 'em all: bending the rules of web cache exploitation - Martin Doyhenard
DC - (11:30-12:15 PDT) - QuickShell: Sharing is caring about an RCE attack chain on Quick Share - Or Yair,Shmuel Cohen
DC - cont...(10:30-11:15 PDT) - Smishing Smackdown: Unraveling the Threads of USPS Smishing and Fighting Back - S1nn3r

DC - (11:30-12:15 PDT) - Sudos and Sudon’ts - Peering inside Sudo for Windows - Michael "mtu" Torres
DC - SHIM me what you got - Manipulating Shim and Office for Code Injection - Ron Ben-Yizhak,David Shandalov
DC - cont...(10:00-11:45 PDT) - CULT OF THE DEAD COW & Friends Present: Prime Cuts from Hacker History - 40 Years of 31337 - Deth Veggie,Walter J. Scheirer,Patrick “Lord Digital” Kroupa,John Threat,Emmanuel Goldstein,X,TommydCat
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DCGVR - Breaking and Defending Cloud Infrastructure: Red Team Evasion Tactics and Access Control Solutions - Amal Joy,Abhishek S
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - cont...(10:00-11:45 PDT) - Maestro - Chris Thompson
DL - cont...(10:00-11:45 PDT) - Tempest - Kirk Trychel
DL - cont...(10:00-11:45 PDT) - 5Ghoul Framework - 5G NR Attacks & 5G OTA Fuzzing - Matheus Eduardo Garbelini,Sudipta Chattopadhyay
DL - cont...(10:00-11:45 PDT) - Testbed Virtual Factory - Borja Pintos Castro,Camilo Piñón Blanco
DL - cont...(10:00-11:45 PDT) - Cyber Security Transformation Chef (CSTC) - Florian Haag,Matthias Göhring
DL - cont...(10:00-11:45 PDT) - MITRE Caldera - Mark Perry,Rachel Murphy
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - Ham Radio Exams -
HRV - Ham Radio for Hackers - Dan "dan_kb6nu" Romanchik
ICSV - Where's Waldo? Can you find the Raspberry Pi in the Cyber Defense Exercise? - Shane McFly,Brian Howard
IOTV - cont...(10:30-11:15 PDT) - Psychic Paper: Making eink access badges accessible for anyone - Joshua Herman
IOTV - (11:15-11:59 PDT) - What To Expect When You’re Exploiting: Attacking and Discovering Zero-Days in Baby Monitors and Wi-Fi Cameras - Eric Forte,Mark Mager
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:15-11:45 PDT) - Learn BadUSB Hacking With the USB Nugget - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - Hack the Badge (Badge class level 2) (Overflow if Friday is too full) -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -

MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-12:59 PDT) - Resume Reviews -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - cont...(10:30-11:30 PDT) - Protecting the Backbone of Our Modern World - Soledad Antelada Toledano
MISC - (11:30-12:30 PDT) - Cybersecurity for Emerging Tech (panelists would include researchers or industry executives in emerging tech categories, like space, OT, hardware like drones, etc) - Paulino Calderon
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - Introduction to IPv6 - Denis Smajlović
PLV - How can hackers support efforts to secure AI systems? - Wan Ding Yao,Christine Lai,Anjuli Shere
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - Social Engineering Improv Acting Techniques - Tim Roberts
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - (11:30-12:10 PDT) - Emulating Magstripe with Arduino - Leigh-Anne Galloway
QTV - Hacking Quantum Key Distribution (QKD) - Vadim Makarov
RCV - cont...(10:00-11:59 PDT) - Maltego Community Workshop - Carlos Fragoso
RCV - cont...(10:00-13:59 PDT) - Recon Village GE(O)SINT Challenge -
RCV - Interview - RedHunt Labs (Kunal), Hosted by Anant Shrivastava - RedHunt Labs (Kunal),Anant Shrivastava
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(10:30-11:25 PDT) - RF CTF Kick Off Day 2 - RF Hackers
RFV - (11:30-12:30 PDT) - AMA on Proxmark3 with Iceman - Iceman
RTV - OSINT for Hackers - Lee McWhorter,Sandra Stibbards
RTV - Securing the Future with CoSAI: Identified Technical Workstreams and Call for Contributions - Omar Santos,Dan McInerney,Daniel Rohrer,Jay White,Paul Vixie,Sarah Novotny
RTV - Developing Evilginx Phishlets - Michael Donley
RTV - RustOps - Jose Plascencia
RTV - Island Hoping: Move from LOLBins to Living off Langs - Moses Frost
SEV - cont...(10:00-12:30 PDT) - John Henry Competition - Human vs. AI & Panel Discussion -
SEV - cont...(10:00-17:59 PDT) - Social Engineering Community Village Hours -
TCV - GPON Unplugged - Akib Sayyed
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - Democracy From Around the World - Harri Hursti
VMV - First Time TSX Hacking Challenge - Tailor Tolliver
VMV - (11:45-12:15 PDT) - The Threat of Deepfakes and Synthetic Media to Election Integrity - Dr. Matthew Canham
WS - cont...(09:00-12:59 PDT) - Sold Out - Sharp Security from All Angles: Mastering Security in .NET Core 8 and Angular 17 Applications - Or Sahar,Yariv Tal
WS - cont...(09:00-12:59 PDT) - Sold Out - Hacking The Metal: A Spark of Intelligence - eigentourist
WS - cont...(09:00-12:59 PDT) - Sold Out - Capture the Flag 101 - Micah Silverman
WS - cont...(09:00-12:59 PDT) - Sold Out - Hacking Apps on Salesforce - Rodney David Beede
WS - cont...(09:00-12:59 PDT) - Sold Out - Industrial Control Systems: how to secure them in practice! - Alexandrine

Torrents
XRV - (11:30-11:59 PDT) - Student Engagement Doesn't Have to Suck - Dr. Muhsinah Morris
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - AR + Art = interactive installations to bring your stories to life - Zaire Moore

Saturday - 12:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - Hands-on Kubernetes security with KubeHound (purple teaming) - Julien Terriac
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - cont...(11:30-12:30 PDT) - garak : A Framework for Large Language Model Red Teaming - Leon Derczynski,Erick Galinkin,Jeffery Martin,Subho Majumdar
APV - cont...(11:00-13:59 PDT) - Application Threat Modeling with Trike - AreTillery
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - cont...(11:40-12:10 PDT) - Unlocking the Gates - Understanding Authentication Bypass Vulnerabilities - Vikas Khanna
APV - (12:20-12:50 PDT) - Maturing Your Application Security Program - SheHacksPurple
APV - cont...(11:00-12:59 PDT) - Activity: Vulnerability Hunt - The Snippets Edition - Mário Leitão-Teixeira
APV - cont...(11:00-12:59 PDT) - Activity: API Security 101: Testing and Trivia by Akto.io - Ankush Jain,Ankita Gupta
APV - cont...(11:00-12:59 PDT) - Activity: Capture the Container by Chainguard - Jonathan Leitschuh
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - Secure the Skies: A Modern Android Security Research Framework for Drone Ground Control Stations and Applications - Jonathan Waterman
ASV - (12:30-12:59 PDT) - GPS spoofing: it's about time, not just position - Ken Munro
BBV - cont...(11:00-12:30 PDT) - The Bug Hunters Methodology Live - DEF CON Edition - Jason Haddix
BBV - (12:30-13:59 PDT) - A Bug Hunter's Guide to Account Takeover - Ben "NahamSec" Sadeghipour
BBV - cont...(11:30-12:30 PDT) - Hunters and Gatherers: A Deep Dive into the World of Bug Bounties - Johnathan Kuskos,Katie Trimble-Noble,Sam (erbbysam) Erb,Jeff Guerra,Logan MacLaren
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - cont...(11:30-12:15 PDT) - My Smart Red Team Copilot - Gaspard Baye
BICV - (12:15-12:59 PDT) - Weaponized Convenience: Inside the Rise of Remote Tool Abuse - Nader Zaveri,Fernando Tomlinson
BTV - (12:30-13:30 PDT) - Introduction to Creating Osquery Extensions: Enhancing Endpoint Security Visibility - Kivanc Aydin
BTV - cont...(11:15-12:15 PDT) - Use opensource AI to map alerts & logs into techniques, clusters, and killchains - Ezz Tahoun
BTV - (12:30-13:30 PDT) - From CTI to Creating Campaigns - Noah Lazzaro
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -

CLV - cont...(11:50-12:15 PDT) - One Click, Six Services: Abusing The Dangerous Multi-service Orchestration Pattern - Liv Matan
CLV - (12:15-12:40 PDT) - Finding Holes in Conditional Access Policies - Brandon Colley
CLV - (12:40-13:10 PDT) - Revealing Choke Points: Practical Tactics for Boosting Cloud Security - Filipi Pires
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC’s Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-16:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:00-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-15:59 PDT) - A Wall of Bribes -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-12:59 PDT) - Live Recon Contest in Progress -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(10:00-16:59 PDT) - Red Alert ICS CTF -
CON - cont...(11:00-12:59 PDT) - DEF CON 32 Beard and Mustache Contest -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CPV - (12:30-12:59 PDT) - Basic Mobile Phone Privacy - Grey Fox

DC - Disenshittify or die! How hackers can seize the means of computation and build a new, good internet that is hardened against our asshole bosses' insatiable horniness for enshittification. - Cory Doctorow
DC - cont...(11:30-12:15 PDT) - QuickShell: Sharing is caring about an RCE attack chain on Quick Share - Or Yair,Shmuel Cohen
DC - (12:30-13:15 PDT) - The Secret Life of a Rogue Device - Lost IT Assets on the Public Marketplace - Matthew "mandatory" Bryant
DC - cont...(11:30-12:15 PDT) - Sudos and Sudon’ts - Peering inside Sudo for Windows - Michael "mtu" Torres
DC - (12:30-13:15 PDT) - AMD Sinkclose: Universal Ring -2 Privilege Escalation - Enrique Nissim,Krzysztof Okupski
DC - Grand Theft Actions: Abusing Self-Hosted GitHub Runners at Scale - Adnan Khan,John Stawinski
DC - The wild and wonderful world of early Microprocessors (with a focus on the 6502) - Michael Brown
DC - automobiles, alcohol, blood, sweat, and creative reversing of an obfuscated Car-Modding tool - atlas
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DCGVR - DEF CON Groups Panel #1 - ET E,xray,TX,overcast,Abhishek S
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - Open Hardware Design for BusKill Cord - Melanie Allen
DL - The Metasploit Framework v6.4 - Jack Heysel,Spencer McIntyre
DL - CODASM - Hiding Payloads in Plain .text - Moritz Laurin Thomas
DL - GC2 - The First Serverless Command & Control - Lorenzo Grazian
DL - MPT - Pentest in Action - Jyoti Raval
DL - FACTION - Josh Summitt
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - HDA Presents the open Synth Jam Session -
HRV - cont...(11:00-16:59 PDT) - Ham Radio Exams -
ICSV - I am still the Captain now! - Paul Brownridge
ICSV - (12:30-12:59 PDT) - Manufacturing- Lessons Learned, Lessons Taught - Tim Chase
ICSV - Don't Give Up The Ship! Maritime SOC/NOC Afloat - Philip Acosta,Cliff Neve,Brad Proctor
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - LoRa for Hackers : Long Range Hacking for Beginners With CircuitPython - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
LPV - Dozier Drill Tournament -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -

MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - Austin School For The Driven -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-12:59 PDT) - Resume Reviews -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - 3D Printing My Way to Sanity: The Self-Funding Hobby That Changed Everything - Steve Dossey
MISC - cont...(11:30-12:30 PDT) - Cybersecurity for Emerging Tech (panelists would include researchers or industry executives in emerging tech categories, like space, OT, hardware like drones, etc) - Paulino Calderon
MISC - (12:30-13:30 PDT) - Threats in Space: The Dangerous Rise of GNSS Attacks - Isabel Manjarrez
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PLV - (12:30-13:15 PDT) - Pick Your Poison: Navigating a secure clean energy transition - Emma Stewart
PLV - cont...(11:00-12:20 PDT) - How can hackers support efforts to secure AI systems? - Wan Ding Yao,Christine Lai,Anjuli Shere
PLV - (12:30-12:50 PDT) - Measuring the international balance of trade in Internet bandwidth: introducing Netflow to Ministries of Finance - Bill Woodcock
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - cont...(11:00-12:59 PDT) - Social Engineering Improv Acting Techniques - Tim Roberts
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - cont...(11:30-12:10 PDT) - Emulating Magstripe with Arduino - Leigh-Anne Galloway
QTV - Threat Modelling QKD -
RCV - cont...(10:00-13:59 PDT) - Recon Village GE(O)SINT Challenge -
RCV - Interview - Daniel Miessler, Hosted by Ankur - Daniel Miessler,Ankur
RCV - OWASP Amass Expanding Data Horizons: Amassing More Than Subdomains - Jeff Foley
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - cont...(11:30-12:30 PDT) - AMA on Proxmark3 with Iceman - Iceman
RFV - (12:30-12:55 PDT) - DoorSim - making my conference travel easier - evildaemond (Adam Foster)
RTV - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - Insert coin: Hacking arcades for fun - Ignacio Daniel Navarro
RTV - Developing Better Payloads with Automated Testing - Nick McClendon
RTV - Tunnel Vision: Exploring VPN Post-Exploitation Techniques - Ori David
SEV - cont...(10:00-17:59 PDT) - Social Engineering Community Village Hours -
SEV - cont...(10:00-12:30 PDT) - John Henry Competition - Human vs. AI & Panel Discussion -
SEV - (12:30-12:59 PDT) - SECV - Break / Networking -
SOC - Friends of Bill W -
TCV - cont...(11:00-13:59 PDT) - GPON Unplugged - Akib Sayyed
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -

VMV - cont...(11:45-12:15 PDT) - The Threat of Deepfakes and Synthetic Media to Election Integrity - Dr. Matthew Canham
VMV - (12:15-13:15 PDT) - Indivisible - Michael Moore
WS - cont...(09:00-12:59 PDT) - Sold Out - Sharp Security from All Angles: Mastering Security in .NET Core 8 and Angular 17 Applications - Or Sahar,Yariv Tal
WS - cont...(09:00-12:59 PDT) - Sold Out - Hacking The Metal: A Spark of Intelligence - eigentourist
WS - cont...(09:00-12:59 PDT) - Sold Out - Capture the Flag 101 - Micah Silverman
WS - cont...(09:00-12:59 PDT) - Sold Out - Hacking Apps on Salesforce - Rodney David Beede
WS - cont...(09:00-12:59 PDT) - Sold Out - Industrial Control Systems: how to secure them in practice! - Alexandrine Torrents
XRV - XR for All: Accessibility and Privacy for Disabled Users - Dylan Fox
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - cont...(11:00-12:59 PDT) - AR + Art = interactive installations to bring your stories to life - Zaire Moore

Saturday - 13:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(12:00-13:59 PDT) - Hands-on Kubernetes security with KubeHound (purple teaming) - Julien Terriac
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - (13:30-14:30 PDT) - ConfusedPilot: Data Corruption and Leakage by Misusing Copilot for Microsoft 365 - Ayush RoyChowdhury,Mulong Luo,Mohit Tiwari
APV - Arsenal: SanicDNS - Jasper Insinger
APV - cont...(11:00-13:59 PDT) - Application Threat Modeling with Trike - AreTillery
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - Transforming AppSec: Protecting 'Everything as Code' & Emerging Tech - Kunal Bhattacharya,Sara Attarzadeh,Shahar Man,Trupti Shiralkar
APV - Activity: Spot the Reachable by Backslash - Czesia Glik,Yossi Pik
APV - Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - mcdwayne
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - (13:30-14:30 PDT) - Open Source Drone Hacking Simulator - Nick Aleks,Rudy Mendoza
ASV - Fly Catcher - How I Developed a Low-Cost Raspberry Pi Based Device for ADS-B Spoof - Angelina Tsuboi
ASV - (13:30-13:59 PDT) - Small Satellite Modeling and Defender Software - Kyle Murbach
BBV - cont...(12:30-13:59 PDT) - A Bug Hunter's Guide to Account Takeover - Ben "NahamSec" Sadeghipour
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - Virtual SIEM/SOAR Workshop - Kenneth Ellington
BICV - Navigating Microaggressions and Fostering Inclusive Communication with Peers and Leadership for Black Professionals - Jessica Hoffman
BTV - cont...(12:30-13:30 PDT) - Introduction to Creating Osquery Extensions: Enhancing Endpoint Security Visibility - Kivanc Aydin
BTV - cont...(12:30-13:30 PDT) - From CTI to Creating Campaigns - Noah Lazzaro
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(12:40-13:10 PDT) - Revealing Choke Points: Practical Tactics for Boosting Cloud Security - Filipi Pires
CLV - Runtime Reachability: Prioritizing Vulnerabilities with eBPF & Continuous Profiling - Sam "Frenchie" Stewart
CLV - (13:50-15:50 PDT) - Connecting the Dots: Mastering Alert Correlation for Proactive Defense in the Cloud - Ezz Tahoun
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -

CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(12:00-17:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-16:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:00-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-15:59 PDT) - A Wall of Bribes -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - Live Recon Finalist Selection Process -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - Hacking Boundary Terminal -
CON - cont...(10:00-16:59 PDT) - Red Alert ICS CTF -
CON - Hack3r Runw@y -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CPV - CPV: Intro to Cyphers -
DC - Fireside Chat with Jay Healey and National Cyber Director Harry Coker, Jr. - Harry Coker Jr.,Jay Healey
DC - cont...(12:30-13:15 PDT) - The Secret Life of a Rogue Device - Lost IT Assets on the Public Marketplace - Matthew "mandatory" Bryant
DC - (13:30-14:15 PDT) - NTLM - The Last Ride - Jim Rush,Tomais Williamson
DC - cont...(12:30-13:15 PDT) - AMD Sinkclose: Universal Ring -2 Privilege Escalation - Enrique Nissim,Krzysztof Okupski

DC - (13:30-14:15 PDT) - Behind Enemy Lines: Engaging and Disrupting Ransomware Web Panels - Vangelis Stykas
DC - OH-MY-DC: Abusing OIDC all the way to your cloud - Aviad Hahami
DC - All Your Keyboards Are Belong to US! - Federico Lucifredi
DC - Learn Zero Trust Network Security with Cloudflare -
DC - Inside the FBI's Secret Encrypted Phone Company 'Anom' - Joseph Cox
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DCGVR - cont...(12:05-13:05 PDT) - DEF CON Groups Panel #1 - ET E,xray,TX,overcast,Abhishek S
DCGVR - The Sand Castle - The State of the MacOS Sandbox - Jonathan "JBO" Bar Or
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - cont...(12:00-13:45 PDT) - Open Hardware Design for BusKill Cord - Melanie Allen
DL - cont...(12:00-13:45 PDT) - The Metasploit Framework v6.4 - Jack Heysel,Spencer McIntyre
DL - cont...(12:00-13:45 PDT) - CODASM - Hiding Payloads in Plain .text - Moritz Laurin Thomas
DL - cont...(12:00-13:45 PDT) - GC2 - The First Serverless Command & Control - Lorenzo Grazian
DL - cont...(12:00-13:45 PDT) - MPT - Pentest in Action - Jyoti Raval
DL - cont...(12:00-13:45 PDT) - FACTION - Josh Summitt
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(12:00-15:59 PDT) - HDA Presents the open Synth Jam Session -
HRV - cont...(11:00-16:59 PDT) - Ham Radio Exams -
HRV - Staying alive off the grid - using APRS and Lambdas to monitor temperature remotely - Kamikazi
ICSV - Don't Ship Your Bridges! Tools to Explore Wireless Attack Surfaces in Every Ship's Marine Navigation Systems - Nick Halt,Duncan Woodbury
ICSV - (13:30-13:55 PDT) - The perma-lag: why industrial cybersecurity will never be state-of-the-art - Kyle McMillan
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(12:00-13:59 PDT) - LoRa for Hackers : Long Range Hacking for Beginners With CircuitPython - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
LPV - cont...(12:00-14:59 PDT) - Dozier Drill Tournament -
LPV - Locksport Competitions: Compete in the Olympics of Locks - Matt Burrough
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - (13:30-14:15 PDT) - How we built our REDACTED THING this year, 5n4ck3y, && AMA Panel on Making Badges - AND!XOR

MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Don't go too far… your job is not done! - Chris Cleary
MISC - cont...(12:30-13:30 PDT) - Threats in Space: The Dangerous Rise of GNSS Attacks - Isabel Manjarrez
MISC - (13:30-14:30 PDT) - DarkGate: Cazando a la amenaza y exponiendo su infraestructura - Nestor Sánchez
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PLV - cont...(12:30-13:15 PDT) - Pick Your Poison: Navigating a secure clean energy transition - Emma Stewart
PLV - (13:15-13:59 PDT) - Hacker vs AI: perspectives from an ex-spy - Harriet Farlow
PLV - Global Perspectives in Cybersecurity: Challenging Norms and Expanding Horizons - Wouter Veenstra,Randy Pestana,Kerry-Ann Barrett,Brett DeWitt
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - Smart Shopping Cart Wheels - How they Work - Joseph
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - Breaking software protected crypto implementations - Adrian Garcia
RCV - cont...(10:00-13:59 PDT) - Recon Village GE(O)SINT Challenge -
RCV - cont...(12:00-13:59 PDT) - OWASP Amass Expanding Data Horizons: Amassing More Than Subdomains - Jeff Foley
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - Exploring the Cosmos: Hackable Innovations at the Allen Telescope Array - Luigi Cruz
RTV - cont...(12:00-16:59 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - An Operator's Guide: Hunting SCCM in the Real World - Garrett Foster,Zachary Stein
RTV - macOS Red Team on Corporate Scenarios - Ricardo L0gan
RTV - Building Surgical Implants: A Comprehensive Guide to APT-style Techniques - John Rodriguez
SEV - cont...(10:00-17:59 PDT) - Social Engineering Community Village Hours -
SEV - Cold Calls -
TCV - cont...(11:00-13:59 PDT) - GPON Unplugged - Akib Sayyed
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - cont...(12:15-13:15 PDT) - Indivisible - Michael Moore
VMV - (13:15-13:59 PDT) - Stanford Digital Observatory - Renée DiResta
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -

Saturday - 14:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - CopyCat: An Artist Guide to Adversary Forgery - Cat Self
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - cont...(13:30-14:30 PDT) - ConfusedPilot: Data Corruption and Leakage by Misusing Copilot for Microsoft 365 - Ayush RoyChowdhury,Mulong Luo,Mohit Tiwari
AIV - (14:30-14:59 PDT) - Evaluations and Guardrails against Prompt Injection attacks on LLM powered-applications - Cyrus Nikolaidis,Faizan Ahmad
AIxCC - The Cat-and-Mouse Game of Adversarial Artificial Intelligence - Alvaro Velasquez
AIxCC - (14:30-14:59 PDT) - Establishing the first Open Source Program Office at a United States Federal Agency - Remy DeCausemaker
APV - cont...(13:00-14:30 PDT) - Arsenal: SanicDNS - Jasper Insinger
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - Web2 Meets Web3: Hacking Decentralized Applications - Peiyu Wang
APV - (14:40-15:10 PDT) - Engineers & Exploits: The Quest for Security - Andra,Spyros Gasteratos
APV - cont...(13:00-14:59 PDT) - Activity: Spot the Reachable by Backslash - Czesia Glik,Yossi Pik
APV - cont...(13:00-14:59 PDT) - Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - mcdwayne
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(13:30-14:30 PDT) - Open Source Drone Hacking Simulator - Nick Aleks,Rudy Mendoza
ASV - (14:15-14:59 PDT) - RF Attacks on Aviation's Last Line of Defense Against Mid-Air Collisions (TCAS II) - Giacomo Longo,Vincent Lenders
BBV - (14:30-15:59 PDT) - High ROI Manual Bug Hunting Techniques - Justin "Rhynorater" Gardner
BBV - Efficient Bug Bounty Automation Techniques - Gunnar Andrews
BBV - (14:30-15:15 PDT) - Leveraging AI for Smarter Bug Bounties - Diego Jurado,Joel "Niemand_Sec" Noguera
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BHV - You got a lighter? I need to do some Electroporation. - James Utley,Joshua HIll,Phil Rhodes
BHV - (14:30-15:15 PDT) - The Past, Present, and Future of Bioweapons - Lucas Potter,Meow-Ludo Disco Gamma Meow-Meow ,Xavier Palmer
BICV - How to Find a 0day in iOS Apps - Xavier D. Johnson
BICV - MCPA x BIC x CAPT Virtual National Service Panel 2024 - Sydney Johns,Nikkia Henderson,Manvell Lessane,Dr. William (Bill) Butler,Dr. Juel Tillman

BTV - Store bought is fine, sometimes! - Jason Craig,Lauren Proehl,Tina Velez,William Phillips
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(13:50-15:50 PDT) - Connecting the Dots: Mastering Alert Correlation for Proactive Defense in the Cloud - Ezz Tahoun
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - Gold Bug: Puzzle Panel -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(12:00-17:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC’s Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-16:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:00-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-15:59 PDT) - A Wall of Bribes -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(13:00-15:59 PDT) - Live Recon Finalist Selection Process -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(10:00-16:59 PDT) - Red Alert ICS CTF -
CON - cont...(13:00-14:59 PDT) - Hack3r Runw@y -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -

CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
DC - SQL Injection Isn't Dead: Smuggling Queries at the Protocol Level - Paul Gerste
DC - cont...(13:30-14:15 PDT) - NTLM - The Last Ride - Jim Rush,Tomais Williamson
DC - (14:30-15:15 PDT) - Troll Trapping Through TAS Tools - Exposing Speedrunning Cheaters - Allan "dwangoAC" Cecil
DC - cont...(13:30-14:15 PDT) - Behind Enemy Lines: Engaging and Disrupting Ransomware Web Panels - Vangelis Stykas
DC - (14:30-15:15 PDT) - ACE up the Sleeve: From getting JTAG on the iPhone 15 to hacking into Apple's new USB-C Controller - Thomas "stacksmashing" Roth
DC - Discovering and exploiting local attacks against the 1Password MacOS desktop application - Jeffrey Hofmann,Colby Morgan
DC - cont...(13:00-14:59 PDT) - Learn Zero Trust Network Security with Cloudflare -
DC - Hacking Millions of Modems (and Investigating Who Hacked My Modem) - Sam Curry
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DCGVR - cont...(13:05-14:05 PDT) - The Sand Castle - The State of the MacOS Sandbox - Jonathan "JBO" Bar Or
DCGVR - Brief History of GRC - Allen Baranov
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - MITRE Caldera for OT - Blaine Jeffries,Devon Colmer
DL - Vovk - Advanced YARA Rule Generator v2.0 - Benjamyn Whiteman,Vishal Thakur
DL - TheAllCommander 2.0 - Matthew Handy
DL - Drop-Pi - Doug Kent,Robert Ditmer
DL - Moriarty - Anthony “Coin” Rose,Jake “Hubble” Krasnov
DL - Farming Ndays with GreyNoise - Andrew Morris
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(12:00-15:59 PDT) - HDA Presents the open Synth Jam Session -
HRV - cont...(11:00-16:59 PDT) - Ham Radio Exams -
HRV - Low Power & Long Range Communications - QRP - Escobar
ICSV - Seeing the Unseen: An Evaluation of Active Scanning in ICS Environments - Jennifer Guerra
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - (14:15-16:15 PDT) - Wi-Fi Hacking Self Defense: Four Advanced Techniques and How to Stop Them - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
LPV - cont...(12:00-14:59 PDT) - Dozier Drill Tournament -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - Color Blasted Badge Making: How Hard Could It Be ? - Abhinav Panda,Bradán Lane,Hamster
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - Hard Hat Brigade - Q&A Panel -

MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(13:30-14:15 PDT) - How we built our REDACTED THING this year, 5n4ck3y, && AMA Panel on Making Badges - AND!XOR
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - Friendship Bracelet Making -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - DC Book Club Discussion -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - Resume Reviews -
MISC - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -
MISC - Navigating Bureaucracy: Strategies for a Post-Military Career Encore - Nia Luckey
MISC - cont...(13:30-14:30 PDT) - DarkGate: Cazando a la amenaza y exponiendo su infraestructura - Nestor Sánchez
MISC - (14:30-14:59 PDT) - Make all the things - Construa seus próprios "brinquedos" Threats - Christiane Borges Santos
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PLV - What’s next for the commercial CNE marketplace? A chance for you to influence the policy that will impact the future - UK Repersentative 2,Senior Representative from UK NCSC,Océane Thieriot,Claudi d’Antoine,Bill Marczak,Daniel Cuthbert
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - HandPwning: “Your Hand is your Passport. Verify me. Now let me in!” - Luca "CYBERANTANI" Bongiorni
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
QTV - QML - Quantum Machine Learning: What is it, where did it come from, and how do I start? - Josh Izaac
QTV - (14:45-15:30 PDT) - Playing with Quantum: wayfinding with quantum game theory - Michael Dascal
RCV - ToolMakers Hackathon -
RCV - The art of Pivoting in OSINT Investigations - Ram Ganesh
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - Remote Sensor Node Updates for FISSURE - The RF Framework - Chris Poore
RTV - cont...(12:00-16:59 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - cont...(13:00-14:50 PDT) - An Operator's Guide: Hunting SCCM in the Real World - Garrett Foster,Zachary Stein
RTV - Cloud Offensive Breaches: The Graph-Based Exploitation of Misconfigurations - Filipi Pires
RTV - Tempest c2: Use and Design - Kirk Trychel
RTV - Combining Uncensored and Censored LLMs for Ransomware Generation - Muhammad Mudassar Yamin
SEV - cont...(10:00-17:59 PDT) - Social Engineering Community Village Hours -
SEV - cont...(13:00-14:59 PDT) - Cold Calls -
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - Understanding the Role of Secretary of States in Elections - Dave Scanlan
VMV - (14:45-15:30 PDT) - Understanding Cognitive Warefare in a Geopolitcal Context - Constantine Nicolaidis

WS - Sold Out - Email Detection Engineering and Threat Hunting - Alfie Champion,Josh Kamdjou
WS - Sold Out - Crash Course in Physical Access Control Systems - Lorenzo Pedroncelli,Randy Belbin
WS - Sold Out - Playing with RFID - Vinnie "kernelpaniek" Vanhoecke
WS - Sold Out - Master Class: Hands-On Machine Learning to Enhance Malware Analysis, Classification, and Detection - Solomon Sonya
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -

Saturday - 15:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(14:00-15:59 PDT) - CopyCat: An Artist Guide to Adversary Forgery - Cat Self
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIV - Bridging the Experience Gap in Machine Learning Security - Kellee Wicker (Moderator),Christine Lai,David Lo,Austin Carson,Nick Landers
AIxCC - Contextualizing Open Source Software's Importance to CISA's Mission - Aeva Black
AIxCC - (15:45-16:30 PDT) - A Reverse Engineer's Guide to AI Interpretability - Dr. Andrew Fasano
APV - Injecting and Detecting Backdoors in Code Completion Models - Ori Ron,Tal Folkman
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - cont...(14:40-15:10 PDT) - Engineers & Exploits: The Quest for Security - Andra,Spyros Gasteratos
APV - (15:20-15:50 PDT) - Speed Bumps and Speed Hacks: Adventures in Car Manufacturers Security - David Sopas,Paulo A. Silva
APV - Activity: Spot the Reachable by Backslash - Czesia Glik,Yossi Pik
APV - Activity: API Security 101: Testing and Trivia by Akto.io - Ankush Jain,Ankita Gupta
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
BBV - cont...(14:30-15:59 PDT) - High ROI Manual Bug Hunting Techniques - Justin "Rhynorater" Gardner
BBV - cont...(14:30-15:15 PDT) - Leveraging AI for Smarter Bug Bounties - Diego Jurado,Joel "Niemand_Sec" Noguera
BBV - (15:15-15:59 PDT) - I've got 99 problems but a prompt injection ain't pineapple - Chloé Messdaghi,Kasimir Schulz
BHV - (15:30-16:30 PDT) - D0N0H4RM: Cyber STEM Storytime - Nitin Natarajan,Christian Dameff,Andrew Carney,Matt Hazelett,Erika Cheung
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BHV - cont...(14:30-15:15 PDT) - The Past, Present, and Future of Bioweapons - Lucas Potter,Meow-Ludo Disco Gamma Meow-Meow ,Xavier Palmer
BICV - FuzzLLM: A Fuzzing Framework for Discovering Jailbreak Vulnerabilities in Large Language Models - Ian G. Harris
BTV - Hot SOC Topics for 2024: Feel the Spice! - Carson Zimmerman,Russ McRee,Eric Lippart,Enoch Long
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(13:50-15:50 PDT) - Connecting the Dots: Mastering Alert Correlation for Proactive Defense in the Cloud - Ezz Tahoun
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -

CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(12:00-17:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-16:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:00-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-15:59 PDT) - A Wall of Bribes -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(13:00-15:59 PDT) - Live Recon Finalist Selection Process -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(10:00-16:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
DC - Exploiting the Unexploitable: Insights from the Kibana Bug Bounty - Mikhail Shcherbakov
DC - cont...(14:30-15:15 PDT) - Troll Trapping Through TAS Tools - Exposing Speedrunning Cheaters - Allan "dwangoAC" Cecil
DC - (15:30-16:15 PDT) - HookChain: A new perspective for Bypassing EDR Solutions - Helvio Carvalho Junior
DC - cont...(14:30-15:15 PDT) - ACE up the Sleeve: From getting JTAG on the iPhone 15 to hacking into Apple's new USB-C Controller - Thomas "stacksmashing" Roth
DC - (15:30-16:15 PDT) - Unsaflok: Hacking millions of hotel locks - Lennert Wouters,Ian Carroll
DC - Measuring the Tor Network - Silvia Puglisi,Roger Dingledine

DC - Real life hacking stories (that can't be recorded!) -
DC - A Shadow Librarian in Broad Daylight: Fighting back against ever encroaching capitalism - Daniel Messer
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DCGVR - How I Learned to Stop Worrying and Love the Ban - Manfred
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
DL - cont...(14:00-15:45 PDT) - MITRE Caldera for OT - Blaine Jeffries,Devon Colmer
DL - cont...(14:00-15:45 PDT) - Vovk - Advanced YARA Rule Generator v2.0 - Benjamyn Whiteman,Vishal Thakur
DL - cont...(14:00-15:45 PDT) - TheAllCommander 2.0 - Matthew Handy
DL - cont...(14:00-15:45 PDT) - Drop-Pi - Doug Kent,Robert Ditmer
DL - cont...(14:00-15:45 PDT) - Moriarty - Anthony "Coin" Rose,Jake "Hubble" Krasnov
DL - cont...(14:00-15:45 PDT) - Farming Ndays with GreyNoise - Andrew Morris
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - (15:15-15:59 PDT) - Reverse engineering and hacking Ecovacs robots - Dennis Giese,Braelynn
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HDA - cont...(12:00-15:59 PDT) - HDA Presents the open Synth Jam Session -
HRV - cont...(11:00-16:59 PDT) - Ham Radio Exams -
HRV - Clapping cheeks, aka home brew antennas - Seth
ICSV - War Games: Red Team for OT (Based on Real World Case Studies) - Shishir Gupta
ICSV - Underway to Identifying Commonalities of Cybersecurity Incidents in the Maritime Transportation System - Rebecca J. Rohan
ICSV - (15:30-15:55 PDT) - Building Zero Trust in ICS - Sting
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(14:15-16:15 PDT) - Wi-Fi Hacking Self Defense: Four Advanced Techniques and How to Stop Them - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(14:00-15:45 PDT) - Friendship Bracelet Making -
MISC - (15:45-15:59 PDT) - WISP Group Photo -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -

MISC - cont...(10:00-15:59 PDT) - Retro Repair -
MISC - cont...(10:00-15:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-15:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-15:59 PDT) - Show & Tell -
MISC - cont...(14:00-15:59 PDT) - DC Book Club Discussion -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(14:00-17:59 PDT) - Resume Reviews -
MISC - Name the Noob -
MISC - Cybersecurity for Veterans: Bridging the Gap from Military to Civilian Careers - Matt James
MISC - Ransomware B-Sides: Los ransoms que nunca triunfaron - Mauro Eldritch,Cybelle Oliveira
MISC - (15:30-16:30 PDT) - Haciendo visible lo invisible: Observabilidad y transparencia en routers Draytek - Gastón Aznarez,Octavio Gianatiempo
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PLV - cont...(14:00-15:45 PDT) - What's next for the commercial CNE marketplace? A chance for you to influence the policy that will impact the future - UK Repersentative 2,Senior Representative from UK NCSC,Océane Thieriot,Claudi d'Antoine,Bill Marczak,Daniel Cuthbert
PSV - Bypass 102 - Karen Ng,Terry Luan
PSV - (15:30-15:59 PDT) - Access Control Done Right the First Time - Tim Clevenger
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - (15:30-16:30 PDT) - Intermediate Physical Security - Justin Wynn
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - Online Payments - Attack and Defense - Vincent Sloan
QTV - cont...(14:45-15:30 PDT) - Playing with Quantum: wayfinding with quantum game theory - Michael Dascal
QTV - (15:30-16:30 PDT) - Covert Quantum Communication - Evan Anderson
RCV - cont...(14:00-17:59 PDT) - ToolMakers Hackathon -
RCV - cont...(14:00-15:59 PDT) - The art of Pivoting in OSINT Investigations - Ram Ganesh
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - Current EW techniques - Kent Britain
RFV - (15:30-15:55 PDT) - Who's Afraid of Synthetic Aperture Radar? - Abraxas3d
RTV - cont...(12:00-16:59 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - The Curious Case of Stealer Logs: Access & Espionage in the World's Most Interesting Dataset - Eric Clay,Nick Ascoli
RTV - Introduction to Kubernetes common attack techniques - Lenin Alevski
RTV - Using Retrieval Augmented Generation (RAG), Langchain, and LLMs for Cybersecurity Operations - Omar Santos
RTV - Learning the New Amass Collection Engine - Jeff Foley
SEV - cont...(10:00-17:59 PDT) - Social Engineering Community Village Hours -
SEV - SECV - Break / Networking -
SEV - (15:30-17:30 PDT) - Cold Calls -
TCV - 4G Frenzy - Vinod Shrimali
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - cont...(14:45-15:30 PDT) - Understanding Cognitive Warefare in a Geopolitcal Context - Constantine Nicolaidis
VMV - (15:30-16:30 PDT) - Cognative Weather Report - Constantine Nicolaidis,Catherine Terranova
WS - cont...(14:00-17:59 PDT) - Sold Out - Email Detection Engineering and Threat Hunting - Alfie Champion,Josh Kamdjou
WS - cont...(14:00-17:59 PDT) - Sold Out - Crash Course in Physical Access Control Systems - Lorenzo Pedroncelli,Randy

Belbin
WS - cont...(14:00-17:59 PDT) - Sold Out - Playing with RFID - Vinnie "kernelpaniek" Vanhoecke
WS - cont...(14:00-17:59 PDT) - Sold Out - Master Class: Hands-On Machine Learning to Enhance Malware Analysis, Classification, and Detection - Solomon Sonya
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -

Saturday - 16:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - Cyberjutsu Path to a Digital Martial Art - Alexandre CABROL PERALES,Quentin Fraty,Alaric Becker
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIxCC - cont...(15:45-16:30 PDT) - A Reverse Engineer's Guide to AI Interpretability - Dr. Andrew Fasano
APV - cont...(15:00-16:59 PDT) - Injecting and Detecting Backdoors in Code Completion Models - Ori Ron,Tal Folkman
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - The Missing Link - How we collect and leverage SBOMs - Cassie Crossley
APV - (16:40-17:10 PDT) - 0.0.0.0 Day: Exploiting Localhost APIs From The Browser - Avi Lumelsky,Gal Elbaz
APV - cont...(15:00-16:59 PDT) - Activity: Spot the Reachable by Backslash - Czesia Glik,Yossi Pik
APV - cont...(15:00-16:59 PDT) - Activity: API Security 101: Testing and Trivia by Akto.io - Ankush Jain,Ankita Gupta
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - Choose your own adventure: Has your fleet been hacked? - Ken Munro
ASV - (16:30-16:59 PDT) - Offensive Security Testing: Safeguarding the Final Frontier - Andrzej Olchawa
BBV - Unveiling Vulnerabilities: A Comprehensive Guide to Bug Bounty Recon - Dhiyaneshwaran Balasubramaniam,Prince Chaddha,Tarun Koyalwar
BHV - cont...(15:30-16:30 PDT) - D0N0H4RM: Cyber STEM Storytime - Nitin Natarajan,Christian Dameff,Andrew Carney,Matt Hazelett,Erika Cheung
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BICV - The Transparency Algorithm: AI's Answer to Legal Racial and Social Inequality - Aquarious Workman
BTV - Thrunting or DEATH! (A BTV Panel) - Joe Slowik,Randy Pargman,Sydney Marrone,th3CyF0x,Ryan Chapman
CHV - Exploiting Bluetooth - from your car to the bank account$$ - Vladyslav Zubkov,Martin Strohmeier
CHV - (16:30-16:59 PDT) - Programming a CTS-V Gauge Cluster into an ATS-V, out of pure spite - Varjitt Jeeva
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - Exploiting common vulnerabilities in AWS environments - Seth Art
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -

CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(12:00-17:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-16:59 PDT) - Tinfoil Hat Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-16:59 PDT) - DC Kubernetes Capture the Flag (CTF) -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:00-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - Live Recon Finalist Presentations -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(10:00-16:59 PDT) - Red Alert ICS CTF -
CON - Crash and Compile -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-16:59 PDT) - Blacks in Cyber CTF -
CON - cont...(10:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CPV - A Whirlwind Tour of the FBI's Secret Encrypted Chat App - Joseph Cox
DC - Compromising an Electronic Logging Device and Creating a Truck2Truck Worm - Jake Jepson,Rik Chatterjee
DC - (16:30-17:15 PDT) - Watchers being watched: Exploiting the Surveillance System and its supply chain - Chanin Kim,Myeonghun Pak,Myeongjin Shin
DC - cont...(15:30-16:15 PDT) - HookChain: A new perspective for Bypassing EDR Solutions - Helvio Carvalho Junior
DC - (16:30-17:15 PDT) - DEF CON Academy: Cultivating M4D SK1LLZ In the DEF CON Community - Yan "Zardus" Shoshitaishvili,Perri Adams
DC - cont...(15:30-16:15 PDT) - Unsaflok: Hacking millions of hotel locks - Lennert Wouters,Ian Carroll
DC - (16:30-17:15 PDT) - Breaking the Beam: Exploiting VSAT Satellite Modems from the Earth's Surface - Vincent Lenders,Johannes Willbold,Robin Bisping
DC - Secrets and Shadows: Leveraging Big Data for Vulnerability Discovery at Scale - Bill Demirkapi
DC - Encrypted newspaper ads in the 19th century - The world's first worldwide secure communication system - Elonka

Dunin,Klaus Schmeh
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DCGVR - cont...(15:05-16:05 PDT) - How I Learned to Stop Worrying and Love the Ban - Manfred
DCGVR - Unlocking Hidden Superpowers: Neurodiversity in Infosec - Xavier "rubix1138" Ashe
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(11:00-16:59 PDT) - Ham Radio Exams -
HRV - Ham Radio in an HOA: Radio in the Face of Your Oppressor - Danny Quist
ICSV - Product security considerations for OT security appliances - Brandon Dudley,Robert Landavazo
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(14:15-16:15 PDT) - Wi-Fi Hacking Self Defense: Four Advanced Techniques and How to Stop Them - Kody K
IOTV - (16:30-17:59 PDT) - Meshtastic Meetup - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - Peer-to-Peer Mentoring and Networking with optional Swag, Pin & Sticker Exchange -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(14:00-17:59 PDT) - Resume Reviews -
MISC - cont...(15:00-17:59 PDT) - Name the Noob -
MISC - cont...(15:30-16:30 PDT) - Haciendo visible lo invisible: Observabilidad y transparencia en routers Draytek - Gastón Aznarez,Octavio Gianatiempo
MISC - (16:30-17:59 PDT) - How is GenIA Impacting Cybersecurity: The good, The Bad, and The ugly (Trilingual Panel) - Marco Figueroa
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -

PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - (16:30-16:59 PDT) - Decoding Galah, an LLM Powered Web Honeypot - Adel Karimi
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - cont...(15:30-16:30 PDT) - Intermediate Physical Security - Justin Wynn
PYV - cont...(10:00-16:30 PDT) - Payment Village CTF -
PYV - (16:30-16:59 PDT) - Payment Village CTF Day Two Results -
QTV - cont...(15:30-16:30 PDT) - Covert Quantum Communication - Evan Anderson
QTV - (16:30-17:29 PDT) - The Quantum Ethics and Skills Debates - Bob Gourley,Bruna Shinohara de Mendonça,Joan Arrow
QTV - (16:30-17:59 PDT) - Quantum Village Bloch Party! -
RCV - cont...(14:00-17:59 PDT) - ToolMakers Hackathon -
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
RFV - Tracking Real-Time Locations with Rogue WiFi Packets - Mikey Awbrey
RTV - cont...(12:00-16:59 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - Pipeline Pandemonium: How to Hijack the Cloud and Make it Rain - Blake Hudson
RTV - Hacking Policy and Policy Hacking - A Red-Teamer Hacker Guide to the Universe of Cyber Policy - Amit Elazari
RTV - Bespoke C2s are coming of age. - David "Icer" Maynor
RTV - cont...(15:00-16:59 PDT) - Learning the New Amass Collection Engine - Jeff Foley
SEV - cont...(10:00-17:59 PDT) - Social Engineering Community Village Hours -
SEV - cont...(15:30-17:30 PDT) - Cold Calls -
SOC - QueerCon Mixer -
TCV - cont...(15:00-16:59 PDT) - 4G Frenzy - Vinod Shrimali
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - cont...(15:30-16:30 PDT) - Cognative Weather Report - Constantine Nicolaidis,Catherine Terranova
VMV - (16:30-16:59 PDT) - What Do Long Voter Registration Lines Mean? - Jake Braun
WS - cont...(14:00-17:59 PDT) - Sold Out - Email Detection Engineering and Threat Hunting - Alfie Champion,Josh Kamdjou
WS - cont...(14:00-17:59 PDT) - Sold Out - Crash Course in Physical Access Control Systems - Lorenzo Pedroncelli,Randy Belbin
WS - cont...(14:00-17:59 PDT) - Sold Out - Playing with RFID - Vinnie "kernelpaniek" Vanhoecke
WS - cont...(14:00-17:59 PDT) - Sold Out - Master Class: Hands-On Machine Learning to Enhance Malware Analysis, Classification, and Detection - Solomon Sonya
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -

Saturday - 17:00 PDT

Return to Index - Locations Legend

ADV - cont...(10:00-17:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-17:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(16:00-17:59 PDT) - Cyberjutsu Path to a Digital Martial Art - Alexandre CABROL PERALES,Quentin Fraty,Alaric Becker
AIV - cont...(10:00-17:59 PDT) - AI Village Demos -
AIxCC - (17:15-17:59 PDT) - Visualizing AIxCC: Bringing Your Code to Life - Mark Griffin
APV - cont...(10:00-17:30 PDT) - Fix the Flag Wargame - Harley Wilson
APV - cont...(16:40-17:10 PDT) - 0.0.0.0 Day: Exploiting Localhost APIs From The Browser - Avi Lumelsky,Gal Elbaz
APV - (17:20-17:50 PDT) - The Dark Side of Bug Bounty - Jason Haddix
ASV - cont...(10:00-17:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-17:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-17:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-17:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-17:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-17:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-17:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-17:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-17:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-17:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-17:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-17:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - From Theory to Reality: Demonstrating the Simplicity of SPARTA Techniques - Randi Tinney
ASV - (17:30-17:59 PDT) - A dive into world of Aircraft PKI - Matt Gaffney
BBV - Top War Stories from a TryHard Bug Bounty Hunter - Justin "Rhynorater" Gardner
BBV - cont...(16:00-17:30 PDT) - Unveiling Vulnerabilities: A Comprehensive Guide to Bug Bounty Recon - Dhiyaneshwaran Balasubramaniam,Prince Chaddha,Tarun Koyalwar
BBV - (17:30-17:59 PDT) - Meet the PortSwigger Research team (Q/A) - Martin Doyhenard,James "albinowax" Kettle,Gareth Heyes
BHV - cont...(10:00-17:59 PDT) - Biohacking Village: Device Lab -
BTV - Under the Hood: Incident Response at High Speed (A BTV Panel) - Angelo Violetti,David Zito,Nicole Beckwith,Shelly Giesbrecht
CHV - cont...(10:00-17:59 PDT) - Car Hacking Village Activities -
CLV - cont...(16:00-17:59 PDT) - Exploiting common vulnerabilities in AWS environments - Seth Art
CON - cont...(10:00-17:59 PDT) - IoT Village CTF -
CON - cont...(10:00-17:59 PDT) - Cloud Village CTF -
CON - cont...(10:00-17:59 PDT) - Hardware Hacking Village CTF -
CON - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-17:59 PDT) - Embedded CTF -
CON - cont...(10:00-17:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-17:59 PDT) - QOLOSSUS -
CON - cont...(10:00-17:59 PDT) - ICS CTF -
CON - cont...(10:00-17:59 PDT) - Car Hacking Village CTF -

CON - cont...(10:00-17:59 PDT) - HackFortress -
CON - cont...(12:00-17:59 PDT) - Beverage Chilling Contraption Contest -
CON - cont...(10:00-17:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - CrackMeIfYouCan -
CON - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model (DCNTTM) -
CON - cont...(10:00-17:59 PDT) - [CANCELED] AutoDriving CTF -
CON - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-17:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-17:59 PDT) - Hac-Man -
CON - cont...(10:00-17:59 PDT) - Darknet-NG -
CON - cont...(10:00-17:59 PDT) - ? Cube -
CON - cont...(10:00-17:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-17:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-17:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-17:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-17:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-17:59 PDT) - Lonely Tag -
CON - cont...(10:00-17:59 PDT) - spyVspy -
CON - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-17:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(16:00-17:59 PDT) - Live Recon Finalist Presentations -
CON - cont...(10:00-17:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-17:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-17:59 PDT) - Octopus Game -
CON - cont...(10:00-17:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-17:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(13:00-17:59 PDT) - Hacking Boundary Terminal -
CON - cont...(16:00-18:59 PDT) - Crash and Compile -
CON - cont...(10:00-17:59 PDT) - HardWired -
CON - cont...(10:00-17:59 PDT) - Capture the Packet -
CON - cont...(10:30-17:59 PDT) - Blue Team Village CTF -
CON - cont...(10:00-17:59 PDT) - Social Engineering Community Youth Challenge -
CON - cont...(10:00-17:59 PDT) - It's In That Place Where I Put That Thing That Time -
CON - cont...(10:00-17:59 PDT) - venator aurum - A Treasure Hunt -
CPV - Attacks on GenAI data and using vector encryption to stop them - Bob Wall,Patrick Walsh
CPV - (17:30-17:59 PDT) - GUR RIBYHGVBA BS PELCGBTENCUL - Jeff Man
DC - cont...(16:30-17:15 PDT) - Watchers being watched: Exploiting the Surveillance System and its supply chain - Chanin Kim,Myeonghun Pak,Myeongjin Shin
DC - cont...(16:30-17:15 PDT) - DEF CON Academy: Cultivating M4D SK1LLZ In the DEF CON Community - Yan "Zardus" Shoshitaishvili,Perri Adams
DC - cont...(16:30-17:15 PDT) - Breaking the Beam: Exploiting VSAT Satellite Modems from the Earth's Surface - Vincent Lenders,Johannes Willbold,Robin Bisping
DC - (17:30-18:15 PDT) - Iconv, set the charset to RCE: exploiting the glibc to hack the PHP engine - Charles "cfreal" Fol
DC - Techniques for Creating Process Injection Attacks with Advanced Return-Oriented Programming - Bramwell Brizendine,Shiva Shashank Kusuma
DC - (17:30-18:15 PDT) - Nano-Enigma: Uncovering the Secrets Within eFuse Memories - Michal Grygarek,Martin Petran,Hayyan Ali
DC - Quantum Leap: The future of Computing and the security of your online world -
DC - A Treasure Trove of Failures: What History's Greatest Heist Can Teach Us About Defense In Depth - Pete Stegemeyer
DCG - cont...(10:00-17:59 PDT) - DEF CON Groups - Open for questions and hanging out -
DCGVR - cont...(16:05-17:05 PDT) - Unlocking Hidden Superpowers: Neurodiversity in Infosec - Xavier "rubix1138" Ashe
DCGVR - Front line first aid: Triaging your DFIR emergency responders - Neumann "scsideath" Lim
ESV - cont...(10:00-17:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-17:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-17:59 PDT) - Emulating (and Hacking) Embedded Devices -

ESV - cont...(10:00-17:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-17:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-17:59 PDT) - Secure Microcontroller Workshop -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
IOTV - cont...(10:00-17:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-17:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-17:59 PDT) - Hack My TV -
IOTV - cont...(10:00-17:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-17:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-17:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-17:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-17:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-17:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-17:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(16:30-17:59 PDT) - Meshtastic Meetup - Kody K
LPV - cont...(10:00-17:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - cont...(10:00-17:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-17:59 PDT) - All content areas generally open -
MISC - cont...(10:00-17:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-17:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-17:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-17:59 PDT) - Robo Sumo -
MISC - cont...(10:00-17:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(16:00-17:59 PDT) - Peer-to-Peer Mentoring and Networking with optional Swag, Pin & Sticker Exchange -
MISC - cont...(10:00-17:59 PDT) - Game Hacking Community Activities & CTF -
MISC - cont...(10:00-17:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-17:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-17:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-17:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-17:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - cont...(14:00-17:59 PDT) - Resume Reviews -
MISC - cont...(15:00-17:59 PDT) - Name the Noob -
MISC - cont...(16:30-17:59 PDT) - How is GenIA Impacting Cybersecurity: The good, The Bad, and The ugly (Trilingual Panel) - Marco Figueroa
MISC - cont...(10:00-17:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-17:59 PDT) - Botnets -
PHV - cont...(10:00-17:59 PDT) - Packet Inspector -
PHV - cont...(10:00-17:59 PDT) - Linux Trainer -
PHV - cont...(10:00-17:59 PDT) - Packet Detective -
PHV - cont...(10:00-17:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-17:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-17:59 PDT) - Password lab -
PHV - cont...(10:00-17:59 PDT) - FleetDm -
PHV - cont...(10:00-17:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - Exposing Coordinated Attacks Hiding in the Sheer Noise of False Positives and Lone Incidents: A Data Science Correlation and Contextualization Journey of Logs, Events, and Alerts - Ezz Tahoun,Lynn Hamida
PLV - Challenges and Reactions: Cybersecurity and Communications Resilience in Taiwan - Herming Chiueh
PSV - cont...(10:00-17:59 PDT) - Physical Security Village Activities -
PSV - Flipping Locks (The Remix) - Remote Badge Cloning with the Flipper Zero and More - Langston Clement,Dan Goga
QTV - cont...(16:30-17:29 PDT) - The Quantum Ethics and Skills Debates - Bob Gourley,Bruna Shinohara de Mendonça,Joan

Arrow
QTV - cont...(16:30-17:59 PDT) - Quantum Village Bloch Party! -
QTV - (17:15-17:59 PDT) - Bloch Party & More Debates -
RCV - cont...(14:00-17:59 PDT) - ToolMakers Hackathon -
RFV - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
SEV - cont...(10:00-17:59 PDT) - Social Engineering Community Village Hours -
SEV - cont...(15:30-17:30 PDT) - Cold Calls -
SEV - (17:30-17:59 PDT) - Presentation: It Takes a Village... -
SOC - Sticker Swap at DEF CON 32 -
SOC - cont...(16:00-17:59 PDT) - QueerCon Mixer -
SOC - Friends of Bill W -
TEV - cont...(10:00-17:59 PDT) - Tamper Evident Village Activities -
VMV - Misinformation, Disinformation, and Malformation in 2024 - Nicole Tisdale,Michael Moore,Nate Young,Jake Braun,Derek DelGaudio,Kendall Spencer
WS - cont...(14:00-17:59 PDT) - Sold Out - Email Detection Engineering and Threat Hunting - Alfie Champion,Josh Kamdjou
WS - cont...(14:00-17:59 PDT) - Sold Out - Crash Course in Physical Access Control Systems - Lorenzo Pedroncelli,Randy Belbin
WS - cont...(14:00-17:59 PDT) - Sold Out - Playing with RFID - Vinnie "kernelpaniek" Vanhoecke
WS - cont...(14:00-17:59 PDT) - Sold Out - Master Class: Hands-On Machine Learning to Enhance Malware Analysis, Classification, and Detection - Solomon Sonya
XRV - cont...(10:00-17:59 PDT) - Signals Are Everywhere -
XRV - cont...(10:00-17:59 PDT) - ICS Village + XR Village Turn the lights on! -

Saturday - 18:00 PDT

Return to Index - Locations Legend

CON - (18:30-19:30 PDT) - Feet Feud (Hacker Family Feud) -
CON - cont...(16:00-18:59 PDT) - Crash and Compile -
DC - cont...(17:30-18:15 PDT) - Iconv, set the charset to RCE: exploiting the glibc to hack the PHP engine - Charles "cfreal" Fol
DC - cont...(17:30-18:15 PDT) - Nano-Enigma: Uncovering the Secrets Within eFuse Memories - Michal Grygarek,Martin Petran,Hayyan Ali
DCGVR - Something something Meshtastic Pip-Boy Personal Mesh with 150 km reach - Giglio
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - cont...(08:00-18:59 PDT) - Human Registration Open -
MISC - (18:30-21:30 PDT) - EFF Tech Trivia -
SOC - cont...(17:00-18:59 PDT) - Sticker Swap at DEF CON 32 -
SOC - (18:30-22:30 PDT) - Policy Mixer @ DEF CON -

Saturday - 19:00 PDT

Return to Index - Locations Legend

CON - cont...(18:30-19:30 PDT) - Feet Feud (Hacker Family Feud) -
DCGVR - cont...(18:05-19:05 PDT) - Something something Meshtastic Pip-Boy Personal Mesh with 150 km reach - Giglio
DCGVR - Who cashed my check?! Catching (Very Obvious) Fraudsters - Squiddy
DCGVR - (19:35-19:50 PDT) - Shifting left in Reversing apk by converting smali to java - Just Tulpa
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - cont...(18:30-21:30 PDT) - EFF Tech Trivia -
SOC - (19:30-21:59 PDT) - DC Next Gen party -
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -
SOC - Women, gender non-conforming and non-binary meetup with The Diana Initiative -

Saturday - 20:00 PDT

Return to Index - Locations Legend

CON - Hacker Jeopardy -
DCGVR - What!? Is my life that fragile? - hoodiePony
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - cont...(18:30-21:30 PDT) - EFF Tech Trivia -
MISC - DEF CON Movie Night -
SOC - Music Set / Entertainment (Cyberpunk Bar Saturday, ACK Stage) - Wesley McGrew,Syntax (DJ) + Luna (VJ),N8,mattrix,Magik Plan,Kampf
SOC - Hacker Karaoke -
SOC - cont...(19:30-21:59 PDT) - DC Next Gen party -
SOC - Music Set / Entertainment (Pirate's Night For Me! Saturday, SYN Stage) - Skittish and Bus,O'Craven Celtic Pirate Band,Ninjula,Miss Jackalope,Grindhaus Selektor,DJ Scythe,Costume Contest
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -
SOC - cont...(19:00-20:59 PDT) - Women, gender non-conforming and non-binary meetup with The Diana Initiative -
SOC - AIV + BTV Pool Party featuring DUNK-A-FED -

Saturday - 21:00 PDT

Return to Index - Locations Legend

CON - cont...(20:00-21:59 PDT) - Hacker Jeopardy -
HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - Intigriti Hack Shack -
MISC - cont...(18:30-21:30 PDT) - EFF Tech Trivia -
MISC - cont...(20:00-23:59 PDT) - DEF CON Movie Night -
SOC - VETCON -
SOC - cont...(19:30-21:59 PDT) - DC Next Gen party -
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -
SOC - The Illuminati Party -
SOC - RAA for Workgroups 3.11 -
SOC - Jack Rhysider Masquerade Party - Jack Rhysider
SOC - cont...(20:00-23:59 PDT) - AIV + BTV Pool Party featuring DUNK-A-FED -

Saturday - 22:00 PDT

Return to Index - Locations Legend

HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - cont...(20:00-23:59 PDT) - DEF CON Movie Night -
SOC - cont...(18:30-22:30 PDT) - Policy Mixer @ DEF CON -
SOC - cont...(20:00-23:59 PDT) - AIV + BTV Pool Party featuring DUNK-A-FED -

Saturday - 23:00 PDT

Return to Index - Locations Legend

HDA - cont...(10:00-23:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - cont...(20:00-23:59 PDT) - DEF CON Movie Night -
SOC - cont...(20:00-23:59 PDT) - AIV + BTV Pool Party featuring DUNK-A-FED -

Sunday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Sunday - 05:00 PDT

Return to Index - Locations Legend

MISC - Defcon.run -

Sunday - 06:00 PDT

Return to Index - Locations Legend

MISC - cont...(05:00-07:59 PDT) - Defcon.run -

Sunday - 07:00 PDT

Return to Index - Locations Legend

MISC - cont...(05:00-07:59 PDT) - Defcon.run -

Sunday - 08:00 PDT

Return to Index - Locations Legend

MISC - Human Registration Open -
MISC - Lost & Found -

Sunday - 09:00 PDT

Return to Index - Locations Legend

MISC - cont...(08:00-15:59 PDT) - Human Registration Open -
MISC - cont...(08:00-14:59 PDT) - Lost & Found -

Sunday - 10:00 PDT

Return to Index - Locations Legend

ADV - Correlating slow & stealthy APT traces hiding in the sheer noise - Ezz Tahoun
ADV - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - Adversary-Adventure Table-top Game - Adversary Village Crew
AIV - AI Village Demos -
AIV - Photoshop Fantasies - Walter Scheirer
APV - (10:45-12:59 PDT) - Kubernetes Security: Hands-On Attack and Defense - alevsk
APV - Fix the Flag Wargame - Harley Wilson
APV - (10:15-10:45 PDT) - The Immortal Retrofuturism of Mainframe Computers and How to Keep Them Safe - Michelle Eggers
ASV - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - CubeSat Simulator - AMSAT
ASV - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - Darkstar Badge Challenge - Lockheed Martin
ASV - Bricks in the Air -
ASV - ARINC 664 CTF - Boeing
ASV - Detect a Threat - TSA
ASV - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - Space Grand Challenge Luna - CalPoly
ASV - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - PTP Flight Challenge - Pen Test Partners
ASV - Space Systems Security CTF – Platform Security - CT Cubed
ASV - Selfie with a CubeSat - CalPoly
ASV - Drone Capture the Flag (CTF) - Dark Wolf
ASV - Drone Hacking Activity - Dark Wolf
ASV - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - Drone Flying Experience - Dark Wolf
ASV - How to Corrupt Youth to Cyber Focused Space Science - RC Jones
BHV - Biohacking Village: Device Lab -
BICV - (10:30-12:30 PDT) - Ain’t that a Breach: Zero Trust Is the Only Solution! - Dr. Louis DeWeaver III
BTV - (10:30-11:59 PDT) - Blue Team Careers: Do what you love, get paid for it! (A BTV Interactive Panel) - Cyb0rg42,Dani,Shea Nangle,Tennisha Martin,Pete Ortega
CHV - Car Hacking Village Activities -
CLV - Cloud Tripwires: fighting stealth with stealth - Jenko Hwong
CLV - (10:35-11:10 PDT) - Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access - Nick Frichette
CON - IoT Village CTF -
CON - Radio Frequency Capture the Flag -
CON - Embedded CTF -
CON - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - Biohacking Village CTF -
CON - QOLOSSUS -
CON - ICS CTF -
CON - Car Hacking Village CTF -
CON - Chasse Partie Systems CTF -
CON - Gold Bug Challenge -
CON - Gold Bug Challenge -
CON - CrackMeIfYouCan -
CON - Red Team Village CTF -
CON - Pinball High Score Contest -

CON - 5N4CK3Y Contest -
CON - Hac-Man -
CON - Darknet-NG -
CON - ? Cube -
CON - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - PhreakMe presented by HackedExistence -
CON - REALI7Y OVERRUN -
CON - Lonely Hard Drive -
CON - Lonely Tag -
CON - A Wall of Bribes -
CON - DEF CON Scavenger Hunt -
CON - Malware Contests: MARC I & BOMBE -
CON - Adversary Wars CTF -
CON - HTB CTF: Data Dystopia -
CON - Octopus Game -
CON - Cyber Defender - The Game -
CON - CMD+CTRL at DEF CON 32 -
CON - Capture the Packet -
CON - HardWired -
CON - venator aurum - A Treasure Hunt -
CPV - Porn & Privacy - ET
CPV - (10:30-11:30 PDT) - Famous and Not-So-Famous Unsolved Codes - Elonka Dunin,Klaus Schmeh
DC - Splitting the email atom: exploiting parsers to bypass access controls - Gareth Heyes
DC - AWS CloudQuarry: Digging for secrets in public AMIs - Eduard Agavriloae,Matei Josephs
DC - Windows Downdate: Downgrade Attacks Using Windows Updates - Alon Leviev
DC - Unlocking the Gates: Hacking a secure Industrial Remote Access Solution - Moritz Abrell
DC - (10:30-11:15 PDT) - Changing Global Threat Landscape with Rob Joyce and Dark Tangent - Rob Joyce,Jeff "The Dark Tangent" Moss
DC - Taking off the blindfold: Detecting persistent threats on Draytek edge devices - Gastón Aznarez,Octavio Gianatiempo
DC - The not-so-silent type: Breaking network crypto in almost every popular Chinese keyboard app - Jeffrey Knockel,Mona Wang
DCG - DEF CON Groups - Open for questions and hanging out -
DDV - Last chance to pick up drives at the DDV -
ESV - Hardware Hacking: Glitching Lab -
ESV - Secure Microcontroller Workshop -
ESV - 101 Labs: Firmware and Software exploitation -
ESV - 101 Labs: Hardware Lab -
ESV - Emulating (and Hacking) Embedded Devices -
ESV - Wireless & Networking workshop - Alex Kelly
HDA - HDA Community - Open for Accessibility Questions/Help -
HRV - Ham Radio Exams -
ICSV - Countdown to Industrial Extinction - Mike Holcomb
IOTV - Safe Hacking -
IOTV - Phisherman's Wharf - Phishing for Beginners -
IOTV - IoT Village Hacking Playground -
IOTV - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - Keysight CTF Challenge -
IOTV - IoT Security at DEF CON 32 -
IOTV - Hack My TV -
IOTV - Firmware Extraction and Analysis -
IOTV - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -

IOTV - Hardware Hacking GE Appliances -
IOTV - (10:15-11:45 PDT) - Wi-Fi Hacker Hunting - Kody K
LPV - Lockpicking Activities -
MISC - cont...(08:00-15:59 PDT) - Human Registration Open -
MISC - All content areas generally open -
MISC - Vendors and Exhibitors Open -
MISC - Hard Hat Brigade - Community Space Open -
MISC - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - Robo Sumo -
MISC - HHV Rube Goldberg Machine -
MISC - WISP Community & Inclusion Room -
MISC - Secure From Scatch -
MISC - Game Hacking Community Activities & CTF -
MISC - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - Small scale LAN party -
MISC - Retro Repair -
MISC - Show & Tell -
MISC - Dumb Terminal fun -
MISC - LHC Meshtastic Activities and CTF -
MISC - LHC's Unofficial Sticker Swap Table -
MISC - Egor's Keyboard Corner -
MISC - Lonely Hackers Club Community Room Open -
MISC - Threat Hunting + Intelligence, capabilities, skills and capabilities inside the LATAM community - Thiago Bordini,Mauro Eldritch,Zoziel
MISC - cont...(08:00-14:59 PDT) - Lost & Found -
MISC - Open Events for DCNextGen -
PHV - Packet Inspector -
PHV - Packet Detective -
PHV - Network-OS: Be The Cloud -
PHV - Botnets -
PHV - Linux Trainer -
PHV - Python + Packet Analysis + Machine Learning -
PHV - Regular Expressions (RegEx) Trainer -
PHV - Password lab -
PHV - FleetDm -
PSV - Physical Security Village Activities -
PSV - (10:30-11:30 PDT) - Bypass 101 - Karen Ng
QTV - Physical Fundamentals of Quantum Computing - Erez M Abrams
RFV - Radio Frequency Village Events -
RTV - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - From Runners to IdP Admin - Sim Cher Boon
RTV - From Network to Network: Hands-On Pivoting Techniques in Internal Environments - Francisco Canteli
RTV - IDOR in Financial Operations - Ilkin Javadov
RTV - Hacking Processes: Introducing the Redteaming Process Framework: RTPF - Alex Gonzalez,Bobby R
RTV - The Village Peoples' Panel - What Really Goes On in a Village? - Justin,Matt Mayes,muteki,Nina Alli,Savannah "lazzslayer" Lazzara,Tom VanNorman,Jeff "The Dark Tangent" Moss
SEV - SECVC Awards & Competitor Panel + Youth Challenge Awards -
SEV - Social Engineering Community Village Hours -
SOC - (10:30-12:20 PDT) - WarDriver Meetup -
TCV - Telecom Tinkerer CTF -
TEV - Tamper Evident Village Activities -
XRV - Play All the Things -
XRV - Evolution of RF Signal Visualization - From Spectrum Analyzers to Augmented Reality - Suzanne Borders,Jad Meouchy

Sunday - 11:00 PDT

Return to Index - Locations Legend

ADV - Exploiting Voice Cloning in Adversarial Simulation - Mark Foudy
ADV - (11:30-11:59 PDT) - Kubernetes Attack Simulation: The Definitive Guide - Leo Tsaousis
ADV - cont...(10:00-11:59 PDT) - Hands-on Attack and Breach Simulation exercises - Adversary Village Crew
ADV - cont...(10:00-11:59 PDT) - Adversary simulator and purple teaming hands-on booth - Adversary Village Crew
ADV - cont...(10:00-11:59 PDT) - Adversary-Adventure Table-top Game - Adversary Village Crew
ADV - cont...(10:00-11:59 PDT) - Correlating slow & stealthy APT traces hiding in the sheer noise - Ezz Tahoun
AIV - cont...(10:00-12:59 PDT) - AI Village Demos -
AIV - My Conversations with a GenAI-Powered Virtual Kidnapper - Perry Carpenter
AIxCC - (11:30-12:15 PDT) - From research to release: Transferring AIxCC results to open source software - Dr. David A. Wheeler,Jeff Diecks,Chris Aniszczyk
APV - Arsenal: Kubescape - OSS security from left to right and everything in the middle - ben@armosec.io
APV - cont...(10:45-12:59 PDT) - Kubernetes Security: Hands-On Attack and Defense - alevsk
APV - cont...(10:00-12:59 PDT) - Fix the Flag Wargame - Harley Wilson
APV - Gridlock: The Dual-Edged Sword of EV and Solar APIs in Grid Security - Vangelis Stykas
APV - (11:45-12:15 PDT) - Your CI/CD Pipeline Is Vulnerable, But It's Not Your Fault - Elad Pticha,Oreen Livni
APV - Activity: Hacking Developers' Trust – Faking GitHub Contribution by Checkmarx - Tal Folkman,Ori Ron,Mário Leitão-Teixeira
APV - Activity: Threat modelling fun session with OWASP Cornucopia - Andra
APV - Activity: Threat modelling fun session with OWASP Cornucopia - Konstantinos Papapanagiotou
ASV - cont...(10:00-12:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-12:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-12:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-12:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-12:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-12:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-12:59 PDT) - Detect a Threat - TSA
ASV - cont...(10:00-12:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-12:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-12:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-12:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-12:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-12:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-12:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - Watch The Skies: Build Your Own ADS-B receiver - Jim "Gurney" Ross
ASV - (11:30-11:59 PDT) - Warflying in a Cessna - Matt Thomassen,Sean McKeever
BBV - Lost in Translation - WAF Bypasses By Abusing Data Manipulation Processes - Ryan Barnett,Isabella Barnett
BHV - cont...(10:00-12:59 PDT) - Biohacking Village: Device Lab -
BICV - cont...(10:30-12:30 PDT) - Ain't that a Breach: Zero Trust Is the Only Solution! - Dr. Louis DeWeaver III
BTV - cont...(10:30-11:59 PDT) - Blue Team Careers: Do what you love, get paid for it! (A BTV Interactive Panel) - Cyb0rg42,Dani,Shea Nangle,Tennisha Martin,Pete Ortega
CHV - cont...(10:00-12:59 PDT) - Car Hacking Village Activities -
CLV - cont...(10:35-11:10 PDT) - Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access - Nick Frichette
CLV - Creating Azure Policy Compliant Backdoor - Viktor Gazdag
CLV - (11:45-12:20 PDT) - The Rise of the Planet of the Agents: LLM-based AI Agents and Cloud Security APIs - Roberto Rodriguez

CON - cont...(10:00-12:59 PDT) - IoT Village CTF -
CON - cont...(10:00-12:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-12:59 PDT) - Embedded CTF -
CON - cont...(10:00-13:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-12:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-12:59 PDT) - QOLOSSUS -
CON - cont...(10:00-12:59 PDT) - ICS CTF -
CON - cont...(10:00-11:59 PDT) - Car Hacking Village CTF -
CON - cont...(10:00-12:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-11:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-11:59 PDT) - Red Team Village CTF -
CON - cont...(10:00-12:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-11:59 PDT) - 5N4CK3Y Contest -
CON - cont...(10:00-12:59 PDT) - Hac-Man -
CON - cont...(10:00-11:59 PDT) - Darknet-NG -
CON - cont...(10:00-11:59 PDT) - ? Cube -
CON - cont...(10:00-12:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-12:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-12:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-12:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-12:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-12:59 PDT) - Lonely Tag -
CON - cont...(10:00-11:59 PDT) - A Wall of Bribes -
CON - cont...(10:00-11:59 PDT) - DEF CON Scavenger Hunt -
CON - cont...(10:00-12:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-11:59 PDT) - Adversary Wars CTF -
CON - cont...(10:00-12:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-12:59 PDT) - Octopus Game -
CON - cont...(10:00-11:59 PDT) - Cyber Defender - The Game -
CON - cont...(10:00-11:59 PDT) - CMD+CTRL at DEF CON 32 -
CON - cont...(10:00-11:59 PDT) - Capture the Packet -
CON - cont...(10:00-12:59 PDT) - HardWired -
CON - cont...(10:00-12:59 PDT) - venator aurum - A Treasure Hunt -
CPV - cont...(10:30-11:30 PDT) - Famous and Not-So-Famous Unsolved Codes - Elonka Dunin,Klaus Schmeh
DC - (|(MaLDAPtive:¯_(LDAP)_/¯=ObFUsc8t10n) (De-Obfuscation &:=De*te)(!c=tion)) - Daniel Bohannon,Sabajete Elezaj
DC - The hack, the crash and two smoking barrels. (And all the times I (almost) killed an engineer.) - Thomas "Cr0wTom" Sermpinis
DC - Dragon SlayingGuide: Bug Hunting In VMware Device Virtualization - JiaQing Huang,Hao Zheng,Yue Liu
DC - cont...(10:30-11:15 PDT) - Changing Global Threat Landscape with Rob Joyce and Dark Tangent - Rob Joyce,Jeff "The Dark Tangent" Moss
DC - (11:30-12:15 PDT) - Open sesame - or how vulnerable is your stuff in electronic lockers - Dennis Giese,Braelynn
DC - Deception & Counter Deception – Defending Yourself in a World Full of Lies - Tom "Decius" Cross,Greg Conti
DCG - cont...(10:00-12:59 PDT) - DEF CON Groups - Open for questions and hanging out -
ESV - cont...(10:00-12:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-12:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-12:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-12:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-12:59 PDT) - Wireless & Networking workshop - Alex Kelly
ESV - cont...(10:00-12:59 PDT) - Hardware Hacking: Glitching Lab -
HDA - cont...(10:00-14:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-13:30 PDT) - Ham Radio Exams -
HRV - Basic Packet Radio Operation - Jeremy
HRV - (11:30-11:59 PDT) - Advanced Packet Radio Operation - Jeremy
ICSV - Tracking Industrial Advanced Threat Actors Who Aren't Really Advanced Just Skiddies Who Deface PLCs and Have

Bad Manners: Methods and Results - Ron Fabela
IOTV - cont...(10:00-12:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-12:59 PDT) - Hack My TV -
IOTV - cont...(10:00-12:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-12:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-12:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-12:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-12:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-12:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-12:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-12:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-12:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:15-11:45 PDT) - Wi-Fi Hacker Hunting - Kody K
LPV - cont...(10:00-12:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-15:59 PDT) - Human Registration Open -
MISC - cont...(10:00-12:59 PDT) - All content areas generally open -
MISC - cont...(10:00-12:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-12:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - cont...(10:00-12:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-12:59 PDT) - Robo Sumo -
MISC - cont...(10:00-12:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-12:59 PDT) - WISP Community & Inclusion Room -
MISC - cont...(10:00-12:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-12:59 PDT) - Retro Repair -
MISC - cont...(10:00-12:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-12:59 PDT) - Show & Tell -
MISC - cont...(10:00-12:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-12:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-11:59 PDT) - Egor's Keyboard Corner -
MISC - cont...(10:00-11:59 PDT) - LHC's Unofficial Sticker Swap Table -
MISC - cont...(10:00-12:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - Detección de Vulnerabilidades mediante Instrumentación y su Explotación - Asher Davila
MISC - cont...(08:00-14:59 PDT) - Lost & Found -
MISC - cont...(10:00-12:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-13:59 PDT) - Packet Inspector -
PHV - cont...(10:00-13:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-13:59 PDT) - Packet Detective -
PHV - cont...(10:00-13:59 PDT) - Botnets -
PHV - cont...(10:00-13:59 PDT) - Linux Trainer -
PHV - cont...(10:00-13:59 PDT) - Password lab -
PHV - cont...(10:00-13:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-13:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-13:59 PDT) - FleetDm -
PLV - Flying Blind: Navigating the Turbulent Skies of Aviation Cybersecurity Regulation - Mike Weigand,Stuart Wagner
PSV - Physical OSINT - Lukas McCullough
PSV - (11:30-11:59 PDT) - Fitness of Physical Red Teamers - Billy Graydon,Lucas Rooyakkers
PSV - cont...(10:00-12:59 PDT) - Physical Security Village Activities -
PSV - cont...(10:30-11:30 PDT) - Bypass 101 - Karen Ng
PSV - (11:30-11:59 PDT) - HandPwning: “Your Hand is your Passport. Verify me. Now let me in!” - Luca "CYBERANTANI" Bongiorni
QTV - FIDO2 in the Quantum Realm - Nina Bindel,James Howe
RFV - cont...(10:00-12:59 PDT) - Radio Frequency Village Events -

RTV - cont...(10:00-11:50 PDT) - DC NextGen / Youth Challenge Area at Red Team Village - RTV Staff
RTV - The SIEMless Hack: Rewriting Reality with Log Injection - Özgün Kültekin
RTV - Threat hunting like a pentester - Ronald Gonzalez
RTV - Red Team Infrastructure Setup and Automation - Aravind Prakash,Arun Nair,Shebin Mathew
RTV - Supercharge your vuln finding workflow with automated labs: How Ludus made it rain creds from SCCM - Erik Hunstad,Alberto Rodriguez
SEV - cont...(10:00-11:30 PDT) - SECVC Awards & Competitor Panel + Youth Challenge Awards -
SEV - cont...(10:00-13:59 PDT) - Social Engineering Community Village Hours -
SEV - (11:30-13:59 PDT) - Cold Calls -
SOC - cont...(10:30-12:20 PDT) - WarDriver Meetup -
TCV - cont...(10:00-13:59 PDT) - Telecom Tinkerer CTF -
TEV - cont...(10:00-12:59 PDT) - Tamper Evident Village Activities -
XRV - cont...(10:00-11:59 PDT) - Play All the Things -

Sunday - 12:00 PDT

Return to Index - Locations Legend

ADV - Village closing - Adversary Village Crew
AIV - cont...(10:00-12:59 PDT) - AI Village Demos -
AIV - Generative Red Team 2 Readout & Acknowledgements - Sven Cattell,Will Pearce,Jerome Wynne,Sean McGregor,Nicole DeCario,Kent Wilson
AIxCC - cont...(11:30-12:15 PDT) - From research to release: Transferring AIxCC results to open source software - Dr. David A. Wheeler,Jeff Diecks,Chris Aniszczyk
APV - cont...(11:00-12:59 PDT) - Arsenal: Kubescape - OSS security from left to right and everything in the middle - ben@armosec.io
APV - cont...(10:45-12:59 PDT) - Kubernetes Security: Hands-On Attack and Defense - alevsk
APV - cont...(10:00-12:59 PDT) - Fix the Flag Wargame - Harley Wilson
APV - cont...(11:45-12:15 PDT) - Your CI/CD Pipeline Is Vulnerable, But It's Not Your Fault - Elad Pticha,Oreen Livni
APV - (12:30-12:59 PDT) - Using EPSS for Better Vulnerability Management - jgamblin
APV - cont...(11:00-12:59 PDT) - Activity: Hacking Developers' Trust – Faking GitHub Contribution by Checkmarx - Tal Folkman,Ori Ron,Mário Leitão-Teixeira
APV - cont...(11:00-12:59 PDT) - Activity: Threat modelling fun session with OWASP Cornucopia - Andra
APV - cont...(11:00-12:59 PDT) - Activity: Threat modelling fun session with OWASP Cornucopia - Konstantinos Papapanagiotou
ASV - cont...(10:00-12:59 PDT) - spacestudio and spacetower challenges - Exotrail,Hack-A-Sat
ASV - cont...(10:00-12:59 PDT) - Hack-A-Sat Digital Twin - Hack-A-Sat,Cromulence
ASV - cont...(10:00-12:59 PDT) - PTP Flight Challenge - Pen Test Partners
ASV - cont...(10:00-12:59 PDT) - Selfie with a CubeSat - CalPoly
ASV - cont...(10:00-12:59 PDT) - Space Systems Security CTF – Platform Security - CT Cubed
ASV - cont...(10:00-12:59 PDT) - Hack-A-Sat Quals Challenges - Hack-A-Sat,Cromulence
ASV - cont...(10:00-12:59 PDT) - Space Grand Challenge Luna - CalPoly
ASV - cont...(10:00-12:59 PDT) - Drone Capture the Flag (CTF) - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - Drone Hacking Activity - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - Drone Hacking Choose Your Own Adventure - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - Drone Flying Experience - Dark Wolf
ASV - cont...(10:00-12:59 PDT) - A-ISAC Aviation Cybersecurity Challenge - A-ISAC and Embry-Riddle Aeronautical University - Prescott
ASV - cont...(10:00-12:59 PDT) - Defend the Airport CTF - IntelliGenesis and IG Labs
ASV - cont...(10:00-12:59 PDT) - Darkstar Badge Challenge - Lockheed Martin
ASV - cont...(10:00-12:59 PDT) - CubeSat Simulator - AMSAT
ASV - cont...(10:00-12:59 PDT) - Bricks in the Air -
ASV - cont...(10:00-12:59 PDT) - ARINC 664 CTF - Boeing
ASV - cont...(10:00-12:59 PDT) - Detect a Threat - TSA
ASV - cont...(11:00-12:59 PDT) - Watch The Skies: Build Your Own ADS-B receiver - Jim "Gurney" Ross
ASV - The Interplay between Safety and Security in Aviation Systems - Lillian Ash Baker
ASV - (12:30-12:59 PDT) - Behind the Badge: How we used and abused hardware to create the AV badge for DC32 - Adam Batori,Robert Pafford
BBV - cont...(11:00-12:30 PDT) - Lost in Translation - WAF Bypasses By Abusing Data Manipulation Processes - Ryan Barnett,Isabella Barnett
BHV - cont...(10:00-12:59 PDT) - Biohacking Village: Device Lab -
BHV - 3DU: Homo (e)x Machina - Lacey Harbour
BICV - cont...(10:30-12:30 PDT) - Ain't that a Breach: Zero Trust Is the Only Solution! - Dr. Louis DeWeaver III
BICV - (12:30-12:59 PDT) - Exploring Bias in AI-Assisted News - Sydney Johns
BTV - Blue Team Village Closing Ceremonies -
CHV - cont...(10:00-12:59 PDT) - Car Hacking Village Activities -
CLV - cont...(11:45-12:20 PDT) - The Rise of the Planet of the Agents: LLM-based AI Agents and Cloud Security APIs - Roberto Rodriguez
CLV - (12:20-12:40 PDT) - Unexpected Leaks in AWS Transit Gateways - William Taylor

CLV - (12:40-12:59 PDT) - Closing Note -
CON - cont...(10:00-12:59 PDT) - IoT Village CTF -
CON - cont...(10:00-12:59 PDT) - Radio Frequency Capture the Flag -
CON - cont...(10:00-12:59 PDT) - Embedded CTF -
CON - cont...(10:00-13:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-12:59 PDT) - Biohacking Village CTF -
CON - cont...(10:00-12:59 PDT) - QOLOSSUS -
CON - cont...(10:00-12:59 PDT) - ICS CTF -
CON - cont...(10:00-12:59 PDT) - Chasse Partie Systems CTF -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CON - cont...(10:00-12:59 PDT) - Pinball High Score Contest -
CON - cont...(10:00-12:59 PDT) - Hac-Man -
CON - cont...(10:00-12:59 PDT) - Ham Radio Fox Hunt - Ham Radio Village Staff
CON - cont...(10:00-12:59 PDT) - Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge -
CON - cont...(10:00-12:59 PDT) - PhreakMe presented by HackedExistence -
CON - cont...(10:00-12:59 PDT) - REALI7Y OVERRUN -
CON - cont...(10:00-12:59 PDT) - Lonely Hard Drive -
CON - cont...(10:00-12:59 PDT) - Lonely Tag -
CON - cont...(10:00-12:59 PDT) - Malware Contests: MARC I & BOMBE -
CON - cont...(10:00-12:59 PDT) - HTB CTF: Data Dystopia -
CON - cont...(10:00-12:59 PDT) - Octopus Game -
CON - cont...(10:00-12:59 PDT) - HardWired -
CON - cont...(10:00-12:59 PDT) - venator aurum - A Treasure Hunt -
DC - DriverJack: Turning NTFS and Emulated Read-only Filesystems in an Infection and Persistence Vector - Alessandro Magnosi
DC - cont...(11:30-12:15 PDT) - Open sesame - or how vulnerable is your stuff in electronic lockers - Dennis Giese,Braelynn
DC - (12:30-13:15 PDT) - Redefining V2G - How to use your vehicle as a game controller - Timm Lauser,Jannis Hamborg
DC - (12:30-13:15 PDT) - AIxCC Closing Ceremonies - Andrew Carney,Perri Adams
DC - Solving the "Lover, Stalker, Killer" Murder with strings, grep, and Perl - Anthony Kava
DC - (12:30-13:15 PDT) - Clash, Burn, and Exploit: Manipulate Filters to Pwn kernelCTF - Kuan-Ting "HexRabbit" Chen
DCG - cont...(10:00-12:59 PDT) - DEF CON Groups - Open for questions and hanging out -
ESV - cont...(10:00-12:59 PDT) - Hardware Hacking: Glitching Lab -
ESV - cont...(10:00-12:59 PDT) - Secure Microcontroller Workshop -
ESV - cont...(10:00-12:59 PDT) - 101 Labs: Firmware and Software exploitation -
ESV - cont...(10:00-12:59 PDT) - 101 Labs: Hardware Lab -
ESV - cont...(10:00-12:59 PDT) - Emulating (and Hacking) Embedded Devices -
ESV - cont...(10:00-12:59 PDT) - Wireless & Networking workshop - Alex Kelly
HDA - cont...(10:00-14:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-13:30 PDT) - Ham Radio Exams -
ICSV - Building a foundation with the 5 critical controls - Dillon Lee
IOTV - Anyone can hack IoT - a beginner’s guide to hacking your first IoT device - Andrew "DigitalAndrew" Bellini
IOTV - cont...(10:00-12:59 PDT) - Safe Hacking -
IOTV - cont...(10:00-12:59 PDT) - Phisherman's Wharf - Phishing for Beginners -
IOTV - cont...(10:00-12:59 PDT) - Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - Drew Green,John Rodriguez,Ken Pyle
IOTV - cont...(10:00-12:59 PDT) - IoT Village Hacking Playground -
IOTV - cont...(10:00-12:59 PDT) - Keysight CTF Challenge -
IOTV - cont...(10:00-12:59 PDT) - IoT Security at DEF CON 32 -
IOTV - cont...(10:00-12:59 PDT) - Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis -
IOTV - cont...(10:00-12:59 PDT) - Firmware Extraction and Analysis -
IOTV - cont...(10:00-12:59 PDT) - Hardware Hacking GE Appliances -
IOTV - cont...(10:00-12:59 PDT) - Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System -
IOTV - cont...(10:00-12:59 PDT) - Hack My TV -

IOTV - IoT Cat Lamp - Kody K
IOTV - (12:30-12:59 PDT) - Finding 0days in Vilo Home Routers - Ava Petersen,Justin Mott
LPV - cont...(10:00-12:59 PDT) - Lockpicking Activities -
MISC - cont...(08:00-15:59 PDT) - Human Registration Open -
MISC - cont...(10:00-12:59 PDT) - Vendors and Exhibitors Open -
MISC - cont...(10:00-12:59 PDT) - All content areas generally open -
MISC - cont...(10:00-12:59 PDT) - Hard Hat Brigade - Community Space Open -
MISC - Hard Hat Brigade - Group Photo and People's Choice Award -
MISC - cont...(10:00-12:59 PDT) - Hardware Hacking and Soldering Skills Village Open (HHV-SSV) -
MISC - cont...(10:00-12:59 PDT) - Robo Sumo -
MISC - cont...(10:00-12:59 PDT) - HHV Rube Goldberg Machine -
MISC - cont...(10:00-12:59 PDT) - WISP Community & Inclusion Room -
MISC - DCNextGen Awards and Closing Ceremony -
MISC - Game Hacking Community Closing Talk & Awards Ceremony -
MISC - cont...(10:00-12:59 PDT) - Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) -
MISC - cont...(10:00-12:59 PDT) - Small scale LAN party -
MISC - cont...(10:00-12:59 PDT) - Show & Tell -
MISC - cont...(10:00-12:59 PDT) - Dumb Terminal fun -
MISC - cont...(10:00-12:59 PDT) - Retro Repair -
MISC - cont...(10:00-12:59 PDT) - LHC Meshtastic Activities and CTF -
MISC - cont...(10:00-12:59 PDT) - Lonely Hackers Club Community Room Open -
MISC - Abusando de Bitlocker para secuestrar información corporativa | Desde la intrusión hasta el descifrado (i) - Eduardo Chavarro Ovalle
MISC - cont...(08:00-14:59 PDT) - Lost & Found -
MISC - cont...(10:00-12:59 PDT) - Open Events for DCNextGen -
PHV - cont...(10:00-13:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-13:59 PDT) - Botnets -
PHV - cont...(10:00-13:59 PDT) - Linux Trainer -
PHV - cont...(10:00-13:59 PDT) - Packet Detective -
PHV - cont...(10:00-13:59 PDT) - Packet Inspector -
PHV - cont...(10:00-13:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-13:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-13:59 PDT) - FleetDm -
PHV - cont...(10:00-13:59 PDT) - Password lab -
PHV - Winning the Game of Active Directory - Brandon Colley
PSV - cont...(10:00-12:59 PDT) - Physical Security Village Activities -
QTV - Policy and the Quantum: Where do we start? -
RFV - cont...(10:00-12:59 PDT) - Radio Frequency Village Events -
RFV - (12:30-12:59 PDT) - World Wide War Drive Outbrief - RF Hackers,WiGLE Staff
SEV - cont...(10:00-13:59 PDT) - Social Engineering Community Village Hours -
SEV - cont...(11:30-13:59 PDT) - Cold Calls -
SOC - cont...(10:30-12:20 PDT) - WarDriver Meetup -
SOC - Friends of Bill W -
TCV - cont...(10:00-13:59 PDT) - Telecom Tinkerer CTF -
TEV - cont...(10:00-12:59 PDT) - Tamper Evident Village Activities -

Sunday - 13:00 PDT

Return to Index - Locations Legend

AIxCC - (13:15-13:59 PDT) - The Challenge in Building a Challenge -
BICV - Expanding Pathways into the National Cyber Workforce - Ayan Islam
CON - cont...(10:00-13:59 PDT) - DARPA's Artificial Intelligence Cyber Challenge (AIxCC) -
CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
CPV - Wu-Tang is for the Children: How States Laws Intended to Protect Children Raise Other Privacy and Legal Risks - Anthony Hendricks
DC - Your AI Assistant has a Big Mouth: A New Side-Channel Attack - Yisroel Mirsky,Roy Weiss,Daniel Ayzenshteyn,Guy Amit
DC - cont...(12:30-13:15 PDT) - Redefining V2G - How to use your vehicle as a game controller - Timm Lauser,Jannis Hamborg
DC - (13:30-14:15 PDT) - Incubated Machine Learning Exploits: Backdooring ML Pipelines Using Input-Handling Bugs - Suha Sabi Hussain
DC - cont...(12:30-13:15 PDT) - AIxCC Closing Ceremonies - Andrew Carney,Perri Adams
DC - (13:30-14:45 PDT) - Contest Closing Ceremonies and Awards -
DC - cont...(12:30-13:15 PDT) - Clash, Burn, and Exploit: Manipulate Filters to Pwn kernelCTF - Kuan-Ting "HexRabbit" Chen
DC - (13:30-14:15 PDT) - Bringing Down North Korea - Alejandro Caceres
HDA - cont...(10:00-14:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
HRV - cont...(10:00-13:30 PDT) - Ham Radio Exams -
ICSV - Career Development - The Human Element - Kirsten Renner
ICSV - (13:30-13:55 PDT) - Forgetting the Fundamentals? Data Communications: Physical and Logical Explanation - Kevin Manna
IOTV - cont...(12:00-13:30 PDT) - IoT Cat Lamp - Kody K
MISC - cont...(08:00-15:59 PDT) - Human Registration Open -
MISC - Jeitinho Cibernético: A Convergência da Segurança no Brasil e América Latina - Ueric Melo
MISC - cont...(08:00-14:59 PDT) - Lost & Found -
PHV - cont...(10:00-13:59 PDT) - Regular Expressions (RegEx) Trainer -
PHV - cont...(10:00-13:59 PDT) - Python + Packet Analysis + Machine Learning -
PHV - cont...(10:00-13:59 PDT) - FleetDm -
PHV - cont...(10:00-13:59 PDT) - Password lab -
PHV - cont...(10:00-13:59 PDT) - Packet Inspector -
PHV - cont...(10:00-13:59 PDT) - Network-OS: Be The Cloud -
PHV - cont...(10:00-13:59 PDT) - Botnets -
PHV - cont...(10:00-13:59 PDT) - Packet Detective -
PHV - cont...(10:00-13:59 PDT) - Linux Trainer -
QTV - (13:15-14:14 PDT) - QOLOSSUS CONTEST Q-CTF Finals -
SEV - cont...(10:00-13:59 PDT) - Social Engineering Community Village Hours -
SEV - cont...(11:30-13:59 PDT) - Cold Calls -
TCV - cont...(10:00-13:59 PDT) - Telecom Tinkerer CTF -

Sunday - 14:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
DC - Abusing legacy railroad signaling systems - David Meléndez,Gabriela (Gabs) Garcia
DC - cont...(13:30-14:15 PDT) - Incubated Machine Learning Exploits: Backdooring ML Pipelines Using Input-Handling Bugs - Suha Sabi Hussain
DC - cont...(13:30-14:45 PDT) - Contest Closing Ceremonies and Awards -
DC - cont...(13:30-14:15 PDT) - Bringing Down North Korea - Alejandro Caceres
HDA - cont...(10:00-14:59 PDT) - HDA Community - Open for Accessibility Questions/Help -
MISC - cont...(08:00-15:59 PDT) - Human Registration Open -
MISC - cont...(08:00-14:59 PDT) - Lost & Found -
QTV - cont...(13:15-14:14 PDT) - QOLOSSUS CONTEST Q-CTF Finals -

Sunday - 15:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
DC - DEF CON Closing Ceremonies & Awards - Jeff "The Dark Tangent" Moss
MISC - cont...(08:00-15:59 PDT) - Human Registration Open -

Sunday - 16:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
DC - cont...(15:00-17:45 PDT) - DEF CON Closing Ceremonies & Awards - Jeff "The Dark Tangent" Moss

Sunday - 17:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-17:59 PDT) - Gold Bug Challenge -
DC - cont...(15:00-17:45 PDT) - DEF CON Closing Ceremonies & Awards - Jeff "The Dark Tangent" Moss

Speaker List

A-ISAC and Embry-Riddle Aeronautical University - Prescott
A-ISAC and Embry-Riddle Aeronautical University - Prescott
A-ISAC and Embry-Riddle Aeronautical University - Prescott
Aakin Patel
Aapo Oksman
Aaron "dyn" Grattafiori
Aaron Crow
Aaron Levy
Aaron Rosenmund
Aaron Shim
Abhijith “Abx” B R
Abhijith “Abx” B R
Abhinav Panda
Abhishek S
Abhishek S
Abraxas3d
Acid-T
Adam "_whatshisface" Pennington
Adam Batori
Adam Dobell
Adam Robbie
Adam Shostack
AdaZebra
Adel Karimi
Adnan Khan
Adrian Coleșa
Adrian Garcia
Adversary Village Crew
Adversary Village Crew
Adversary Village Crew
Adversary Village Crew
Adversary Village Crew
Adversary Village Crew
Adversary Village Crew
Adversary Village Crew
Adversary Village Crew
Adwiteeya Agrawal
Aeva Black
Aeva Black
Agostino Panico
Akib Sayyed
Akib Sayyed
Akib Sayyed
Alan Villaseñor
Alaric Becker
Alberto Rodriguez
Aleise McGowan
Alejandro Caceres
Alek Amrani
Alessandro Magnosi

alevsk
Alex Delifer
Alex Foley
Alex Gonzalez
Alex Kelly
Alex Kelly
Alex Kelly
Alexander Rubin
Alexandre CABROL PERALES
Alexandrine Torrents
Alexandrine Torrents
Alexandru Lazar
Alfie Champion
Allan "dwangoAC" Cecil
Allen Baranov
Alon Leviev
Alvaro Velasquez
Amal Joy
Amit Elazari
AMSAT
AMSAT
AMSAT
Amul Chaulagain
Ana Aslanishvili
Anand Tiwari
Anand Tiwari
Anant Shrivastava
AND!XOR
Andra
Andra
Andra
Andrew "DigitalAndrew" Bellini
Andrew Carney
Andrew Carney
Andrew Carney
Andrew Case
Andrew Johnson
Andrew M
Andrew Morris
Andrew Tierney
Andrzej Olchawa
Andrzej Olchawa
Angelina Tsuboi
Angelo Violetti
Angus Strom
Anjuli Shere
Ankita Gupta
Ankita Gupta
Ankur
Ankush Jain
Ankush Jain
Anna Bower
Anne Neuberger
Anthony “Coin” Rose
Anthony Hendricks

Anthony Kava
Antoine Carossio
Apurv Singh Gautam
Aquarious Workman
Aravind Prakash
Archwisp
AreTillery
Arjun Gopalakrishna
Armando Aguilar
Arnaud Soullié
Arnold Osipov
Arun Nair
Asher Davila
Asher Davila
Ashley Hiram M.
atlas
Aurora Johnson
Austin Carson
Austin Sellers
Ava Petersen
Avi Lumelsky
Avi McGrady
Aviad Hahami
Ayan Islam
Ayush RoyChowdhury
Babak Javadi
Barrett "pwneip" Darnell
Ben "NahamSec" Sadeghipour
Ben "NahamSec" Sadeghipour
Ben "NahamSec" Sadeghipour
Ben Dechrai
Ben Goerz
Ben Varcoe
ben@armosec.io
Benjamyn Whiteman
Bernhard Sedlmayer
BIC Village Staff
Bill Demirkapi
Bill Marczak
Bill Woodcock
Bill Woodcock
Bill Woodcock
Billy Graydon
Billy Graydon
bkobe
Blaine Jeffries
Blake Hudson
Bleon Proko
Bob Gourley
Bob Wall
Bobby R
Boeing
Boeing
Boeing
Borja Pintos Castro

Brad Proctor
Bradán Lane
Bradley Nash
Braelynn
Braelynn
Bramwell Brizendine
Brandon Colley
Brandon Colley
Brandon Dudley
Brett DeWitt
Brian Howard
Brian Weber
Bruna Shinohara de Mendonça
Bruna Shinohara de Mendonça
Bruno Krauss
Bryan Hance
Bryson Bort
Bryson Bort
C$
c0ldbru
Cale Smith
Call the Cops
CalPoly
CalPoly
CalPoly
CalPoly
CalPoly
CalPoly
Camilo Piñón Blanco
CaptHz
Carlos Fragoso
Carlota Bindner
Carson Zimmerman
Caspian Kilkelly
Cassie Crossley
Cassie Crossley
Cat Self
Catherine J. Ullman
Catherine J. Ullman
Catherine Terranova
Catherine Terranova
Catherine Terranova
CATO Networks
Cecilie Wian
Ceri Coburn
Cesar Ortega Ortega
Cesare Pizzi
Ch33r10
Chad Shortman
Changhyun Park
Chanin Kim
Charles "cfreal" Fol
Charles Waterhouse
Charles Waterhouse
Chirag Savla

Chloé Messdaghi
Chloé Messdaghi
Chloé Messdaghi
Chris Aniszczyk
Chris Cleary
Chris Davis
Chris Gates
Chris Poore
Chris Thompson
Chris Thompson
Chris Wysopal
Christian Dameff
Christiane Borges Santos
Christina Liaghati
Christine Lai
Christine Lai
Christophe Tafani-Dereeper
Claudi d'Antoine
Cliff Neve
Col Travis Hartman
Colbert Zhu
Colby Morgan
Constantine Nicolaidis
Constantine Nicolaidis
Cory Doctorow
Cory Doctorow
Cory Watson
Costume Contest
Costume Contest
Craig Chamberlain
Craig Lester
Cromulence
Cromulence
Cromulence
Cromulence
Cromulence
Cromulence
CT Cubed
CT Cubed
CT Cubed
CTRL / rsm
CtrlAltFu
Cyb0rg42
Cybelle Oliveira
Cybelle Oliveira
Cyrus Nikolaidis
Czesia Glik
Czesia Glik
Czesia Glik
Daemon Chadeau
Dafinga
Daiwei Zhu
Damien Cauquil
Dan "dan_kb6nu" Romanchik
Dan "dan_kb6nu" Romanchik

Dan Berte
Dan Goga
Dan Goga
Dan Gunter
Dan McInerney
Dani
Daniel "Blaklis" Le Gall
Daniel Ayzenshteyn
Daniel Beard
Daniel Bohannon
Daniel Cuthbert
Daniel Cuthbert
Daniel Isler
Daniel Messer
Daniel Miessler
Daniel Rohrer
Danilo Erazo
Danny Quist
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dark Wolf
Dave Scanlan
David "CountZ3r0" Roman
David "Icer" Maynor
David "Icer" Maynor
David Lo
David McDonald
David Meléndez
David Shandalov
David Sopas
David Weston
David Zito
deaddoll
Denis Smajlović
Dennis Giese
Dennis Giese
Dennis Giese
Deral Heiland
Derek DelGaudio
Deth Veggie
Devon Colmer
Dhiyaneshwaran Balasubramaniam
Dhruv Shah
Diego Jurado
Dillon Lee
Dimitri Di Cristofaro

Dirk-jan Mollema
DJ Habbs
DJ Roma
DJ Scythe
DJ St3rling
DJ Vulp
DotOrNot
Doug Kent
Dr. Andrew Fasano
Dr. David A. Wheeler
Dr. Fatou Sankare
Dr. Jennifer Roberts
Dr. Juel Tillman
Dr. Kathleen Fisher
Dr. Kosuke Onishi
Dr. Louis DeWeaver III
Dr. Matt Turek
Dr. Matthew Canham
Dr. Muhsinah Morris
Dr. Renee Wegrzyn
Dr. Stefanie Tompkins
Dr. Susan Coller Monarez
Dr. William (Bill) Butler
Dr. William Corvey
Drew "aNullValue" Stemen
Drew Green
Drew Green
Drew Green
Drew Springall
Drinor Selmanaj
Dual Core
Duane Michael
Duncan Woodbury
Dylan "The Magician" Baklor
Dylan Fox
Eddie Zaneski
Eduard Agavriloae
Eduardo Chavarro Ovalle
Ege Feyzioglu
eigentourist
Elad Pticha
Elad Pticha
Eli McRae
Elizabeth Biddlecome
Elizabeth Eigner
Elonka Dunin
Elonka Dunin
Emanuel Valente
Emile Fugulin
Emma Stewart
Emmanuel Goldstein
Emmanuel Law
Endeavors
Enoch Long
Enrique Nissim

Erez M Abrams
Eric Clay
Eric Clay
Eric Forte
Eric Lippart
Eric Woodruff
Erick Galinkin
Erick Galinkin
Erik Hunstad
Erika Cheung
Erwin Karincic
Escobar
ET
Eugene Rodionov
Evan Anderson
evildaemond (Adam Foster)
Exotrail
Exotrail
Exotrail
Ezra Woods
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Faizan Ahmad
Federico Lucifredi
Felipe Pr0teus
Fernando De La Peña Llaca
Fernando Tomlinson
Filipi Pires
Filipi Pires
Filipi Pires
Fleur van Leusden
Florian Haag
Florian Haag
Francisco Canteli
Francisco Perdomo
Fred Wilmot
Gabriela (Gabs) Garcia
Gal Elbaz
Gareth Heyes
Gareth Heyes
Garrett Foster
Garrett Foster
Gaspard Baye
Gaspard Baye
Gastón Aznarez
Gastón Aznarez
Gaurav Joshi
Gautam Peri
General Paul M. Nakasone
Geoff Horvath
Giacomo Longo

Giglio
Giorgio "gbyolo" Bernardinetti
Golden Richard
Gonçalo Marques Raposo de Magalhães
Graham Helton
Greg Conti
Gregory Carpenter
Grey Fox
Grey Fox
Grey Fox
Grifter
Grind613
Grindhaus Selektor
Guillermo Buendia
Gunnar Andrews
Gustavo Moreira
Gustavo Roberto
Guy Amit
Gwyddia
Hack-A-Sat
Hack-A-Sat
Hack-A-Sat
Hack-A-Sat
Hack-A-Sat
Hack-A-Sat
Hack-A-Sat
Hack-A-Sat
Hack-A-Sat
Hahna Kane Latonick
Hallie Stern
Ham Radio Village Staff
Ham Radio Village Staff
Ham Radio Village Staff
Hamster
Hamster
Hanryeol Park
Hao Zheng
Hare Krishna Rai
Harlan Geer
Harley Geiger
Harley Wilson
Harley Wilson
Harley Wilson
Harri Hursti
Harri Hursti
Harri Hursti
Harriet Farlow
Harriet Farlow
Harriet Farlow
Harrison Richardson
Harry Coker Jr.
Harry Krejsa
Harsha Koushik
Harsha Koushik
Hayyan Ali

HD Moore
Heather Adkins
Heather Adkins
Helvio Carvalho Junior
Herming Chiueh
Himanshu Das
HK
hoodiePony
Hubert Lin
Hyo Jin Lee
Ian Carroll
Ian Foster
Ian G. Harris
Ian Hickey
Iceman
Icetre Normal
Iggy
Ignacio Daniel Navarro
Ignacio Daniel Navarro
Ike Marizu
Ilkin Javadov
ILOVEPIE
Ilyes Beghdadi
int eighty (of Dual Core)
IntelliGenesis and IG Labs
IntelliGenesis and IG Labs
IntelliGenesis and IG Labs
Inti De Ceukelaire
iosifache
Irvin Lemus
Isabel Manjarrez
Isabel Manjarrez
Isabel Straw
Isabella Barnett
Ismail Melih Tas
Itay Cohen
Ivan Evtimov
Jack Cyprus
Jack Heysel
Jack Rhysider
Jacob H Braun
Jacob H Braun
Jacob Oakley
Jacob Shams
Jad Meouchy
Jake “Hubble” Krasnov
Jake “Hubble” Krasnov
Jake Braun
Jake Braun
Jake Jepson
Jake Williams
James "albinowax" Kettle
James "albinowax" Kettle
James Hawk
James Howe

James Utley
Jamie Hardy
Jamie Williams
Jan Trzaskowski
Jannis Hamborg
Jared Dixon
Jared Dygert
Jared Dygert
Jason Butryn
Jason Clinton
Jason Craig
Jason Haddix
Jason Haddix
Jason Romero
Jasper Insinger
Jasper Insinger
Javan Rasokat
Jay Chen
Jay Chen
Jay Healey
Jay White
Jayson E. Street
Jayson E. Street
Jayson E. Street
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff Diecks
Jeff Foley
Jeff Foley
Jeff Guerra
Jeff Man
Jeffery Martin
Jeffrey Hofmann
Jeffrey Knockel
Jen Easterly
jen-ozmen
Jenko Hwong
Jennifer Guerra
Jeremy Banker
Jeremy
Jeremy
Jerome Wynne
Jerome Wynne
Jesika Juarez
Jessica Hoffman
Jessica Sexton
Jeswin Mathai
jgamblin
JiaQing Huang
Jim "Gurney" Ross
Jim Rush
Joan Arrow

Joanna Bitton
Joe "Kingpin" Grand
Joe "securelyfitz" FitzPatrick
Joe Slowik
Joe Slowik
Joe Vest
Joel "Niemand_Sec" Noguera
Johannes Willbold
John "2PAC" Smithberger
John Rodriguez
John Rodriguez
John Rodriguez
John Rodriguez
John Stawinski
John Threat
Johnathan Kuskos
Jon DiMaggio
Jon Marler
Jonathan "JBO" Bar Or
Jonathan Fischer
Jonathan Leitschuh
Jonathan Leitschuh
Jonathan Reiter
Jonathan Waterman
Jonghyuk Song
Jordan Kasper
Jorge Acevedo Canabal
Jose Plascencia
Joseph Cox
Joseph Cox
Joseph
Josh Huff
Josh Isaac
Josh Izaac
Josh Kamdjou
Josh Pyorre
Josh Stroschein
Josh Stroschein
Josh Summitt
Joshua Herman
Joshua HIll
Julia Dewitz-Würzelberger
Julien Terriac
Just Tulpa
Justin "Rhynorater" Gardner
Justin "Rhynorater" Gardner
Justin Mott
Justin Wynn
Justin
Jyoti Raval
Kaitlyn Handelman
Kaleeque Pierce
Kaloyan Velikov
Kamikazi
Kampf

Karan Dwivedi
Karen Ng
Karen Ng
Karen Ng
Karen Ng
Karl Fosaaen
Karthik Tadinada
Kasimir Schulz
Kasimir Schulz
Kasimir Schulz
Kasimir Schulz
Katherina Canales
Kathy Zhu
Katie Trimble-Noble
Kellee Wicker (Moderator)
Kemba Walden
Ken Gannon
Ken Kato
Ken Kato
Ken Munro
Ken Munro
Ken Munro
Ken Pyle
Ken Pyle
Ken Pyle
Kendall Spencer
Kendall Spencer
Kenneth Ellington
Kent Britain
Kent Wilson
Kent Wilson
Kerry-Ann Barrett
Kevin "Kent" Clark
Kevin "Kent" Clark
Kevin Manna
Kevin Mitchell
Kevin Parker
Kirk Trychel
Kirk Trychel
Kirsten Renner
Kivanc Aydin
Klaus Schmeh
Klaus Schmeh
Kody K
Kody K
Kody K
Kody K
Kody K
Kody K
Kody K
Kody K
Kody K
Kody K
Konstantinos Karagiannis
Konstantinos Papapanagiotou

Krzysztof Okupski
Kuan-Ting "HexRabbit" Chen
Kunal Bhattacharya
kvprashant
Kyle McMillan
Kyle Murbach
Lacey Harbour
Langston Clement
Langston Clement
Larry Pesce
Lauren Proehl
Lauren Putvin
Lee McWhorter
Leigh-Anne Galloway
Leigh-Anne Galloway
Leigh-Anne Galloway
Leigh-Anne Galloway
Leigh-Anne Galloway
Lenin Alevski
Lenin Alevski
Lenin Alevski
Lenin Alevski
Lennert Wouters
Leo Tsaousis
Leon Derczynski
Leon Derczynski
Leonardo Pigñer
Leonardo Serrano
Leonidas Vasileiadis
Levone Campbell
Lexie Thach
Lillian Ash Baker
Liv Matan
Lockheed Martin
Lockheed Martin
Lockheed Martin
Logan MacLaren
Lorenzo Grazian
Lorenzo Pedroncelli
Lozaning
Luca "CYBERANTANI" Bongiorni
Luca "CYBERANTANI" Bongiorni
Luca "CYBERANTANI" Bongiorni
Lucas Cioffi
Lucas Philippe
Lucas Philippe
Lucas Potter
Lucas Rooyakkers
Luciano Remes
Luigi Cruz
Lukas McCullough
Luke Koch
Luke McLaren
Lynn Hamida
m1ddl3w4r3

Magik Plan
Manfred
Manvell Lessane
Mar Williams
Marcelo Ribeiro
Marco Figueroa
Marcus Hutchins
Mariia Mykhailova
Marilyn Marks
Mário Leitão-Teixeira
Mário Leitão-Teixeira
Mário Leitão-Teixeira
Mário Leitão-Teixeira
Mark Foudy
Mark Griffin
Mark Mager
Mark Perry
Mark Perry
Mars Cheng
Martin Doyhenard
Martin Doyhenard
Martin Petran
Martin Pratt
Martin Rakhmanov
Martin Strohmeier
Martin Strohmeier
Martin Strohmeier
Mary Kaiser
Matei Josephs
Matheus Eduardo Garbelini
Matt Blaze
Matt Blaze
Matt Burch
Matt Burch
Matt Burrough
Matt Domko
Matt Gaffney
Matt Hazelett
Matt James
Matt Knight
Matt Knight
Matt Mayes
Matt Mayes
Matt Pawloski
Matt Thomassen
Matthew "mandatory" Bryant
Matthew Dixson
Matthew Handy
Matthew Nickerson
Matthew Richard
Matthias Göhring
Matthias Göhring
mattrix
Mauro Eldritch
Mauro Eldritch

Mauro Eldritch
Max "Libra" Kersten
Max "Libra" Kersten
Maya Pavlova
MC Frontalot
mcdwayne
mcdwayne
mcdwayne
Meaghan Neill
Megan Squire
Melanie Allen
Melvin Langvik
Meow-Ludo Disco Gamma Meow-Meow
Micah Silverman
Michael "codingo" Skelton
Michael "mtu" Torres
Michael "v3ga" Aguilar
Michael "v3ga" Aguilar
Michael Brown
Michael Butler
Michael Dascal
Michael Donley
Michael Garcia
Michael Gorelik
Michael Katchinskiy
Michael Moore
Michael Moore
Michael Orlitzky
Michaela Barnett
Michal Grygarek
Michelle Eggers
Mika Devonshire
Mike Holcomb
Mike Holcomb
Mike Larkin
Mike Manrod
Mike Raggo
Mike Ruth
Mike Walker
Mike Weigand
Mikey Awbrey
Mikhail Shcherbakov
Mishaal Khan
Mishaal Khan
Miss Jackalope
Mixæl Swan Laufer
Mixæl Swan Laufer
Mohammed Ilyas Ahmed
Mohit Tiwari
Mona Wang
Moritz Abrell
Moritz Laurin Thomas
Moritz Laurin Thomas
Moses Frost
Moses Frost

Muhammad Mudassar Yamin
Mulong Luo
muteki
Myeonghun Pak
Myeongjin Shin
N8
Nadeem Bagwan
Nader Zaveri
Naomi Brockwell
Nasreen Djouini
Natalie Simpson
Nate Young
Nate Young
Nathan Case
Nathan Sidles
Nestor Sánchez
Neumann "scsideath" Lim
NG Yeow Boon
Nia Luckey
Nick Aleks
Nick Aleks
Nick Ascoli
Nick Ascoli
Nick Draffen
Nick Frichette
Nick Frichette
Nick Halt
Nick Landers
Nick McClendon
Nick Warner
Nicole Beckwith
Nicole DeCario
Nicole DeCario
Nicole Tisdale
Nicole Tisdale
Nikhil "niks" Shrivastava
Nikhil "niks" Shrivastava
Nikhil Mittal
Nikita Kronenberg
Nikki Pope
Nikkia Henderson
Nikkia Henderson
Niklas Lindroos
Nina Alli
Nina Bindel
Ninjula
Niru Ragupathy
Nitin Natarajan
Nivedita (Nivu) Jejurikar
Niyo Little Thunder Pearson
Noah Lazzaro
Numan Ozdemir
O'Craven Celtic Pirate Band
Océane Thieriot
Octavio Gianatiempo

Octavio Gianatiempo
Ofek Itach
Ofir Yakobi
Ohm-I & The NPC Collective
Omar Santos
Omar Santos
Omar Santos
Omar Santos
Omenscan
Or Sahar
Or Yair
Oreen Livni
Oreen Livni
Ori David
Ori Ron
Ori Ron
Ori Ron
overcast
Özgün Kültekin
PankleDank
PatAttack
Patrick “Lord Digital” Kroupa
Patrick Eisenschmidt
Patrick Kiley
Patrick Walsh
Paul Brownridge
Paul Gerste
Paul Roberts
Paul Vixie
Paul Wortman
Paulino Calderon
Paulo A. Silva
Pavel Khunt
Peiter “Mudge” Zatko
Peiyu Wang
Pen Test Partners
Pen Test Partners
Pen Test Partners
Per Thorsheim
Perri Adams
Perri Adams
Perry Carpenter
Pete Ortega
Pete Stegemeyer
Phil Rhodes
Philip Acosta
Philip Stark
Philip Stark
Philip Stark
Prashant Venkatesh
Prince Chaddha
Priyanka Joshi
punkcoder
Quentin Fraty
R.J. McCarley

r1otctrl
R4v3n Bl4ck
Rachael Tubbs
Rachel Cummings
Rachel Cummings
Rachel Murphy
Rachel Murphy
Ralph May
Ralph May
Ram Ganesh
Ram
Randi Tinney
Randy Belbin
Randy Pargman
Randy Pestana
Raunak Parmar
Ravid Mazon
Ravid Mazon
Ravin Kumar
Ray Baeza
Ray Baeza
RC Jones
Rebecca Ford
Rebecca J. Rohan
Rebecca Lively
RedHunt Labs (Kunal)
Relay
Remy DeCausemaker
Renée DiResta
Rewanth Tammana
Rey "Privesc" Bango
RF Hackers
RF Hackers
RF Hackers
Ricardo L0gan
Rich DeMillo
Rick Altherr
Ricky "HeadlessZeke" Lawshae
Rik Chatterjee
Rob Joyce
Rob King
Robert Ditmer
Robert Landavazo
Robert Pafford
Robert Pimentel
Robert Van Etta
Roberto Rodriguez
Roberto Soares
Robin Bisping
Rodney David Beede
Roger Dingledine
Rohit Pitke
Romain Cayre
Ron Ben-Yizhak
Ron Fabela

Ronald Broberg
Ronald Gonzalez
Roni "Lupin" Carta
Roni "Lupin" Carta
Rotem Bar
Roy Weiss
RTV Staff
RTV Staff
RTV Staff
Rudy Mendoza
Ruoyu "Fish" Wang
Rupali
Russ McRee
Ryan Barnett
Ryan Chapman
Ryan Chapman
Ryan Holeman
Ryan Johnson
Ryan M. "0dayCTF" Montgomery
Ryan O'Donnell
Ryan O'Donnell
Ryan Rutan
Ryan Tracey
S1nn3r
Sabajete Elezaj
Salvador Mendonza
Sam "Frenchie" Stewart
Sam (erbbysam) Erb
Sam Bowne
Sam Cosentino
Sam Curry
Sam Mayers
samy kamkar
Sandra Stibbards
Sanne Maasakkers
Sara Attarzadeh
Sarah Hipel
Sarah Mader
Sarah Novotny
Sarthak Taneja
Sarthak Taneja
Savannah "lazzslayer" Lazzara
Savannah "lazzslayer" Lazzara
Scotch & Bubbles
Scott Helme
Scott Weston
Sean
Sean McGregor
Sean McGregor
Sean McKeever
Sean Metcalf
Sean Oesch
Sebastiaan Pierrot
Sebastian Cesario
Sebastian Tapia De la torre

Sebastien Tricaud
Senior Representative from UK NCSC
Serrgei Frankoff
Seth Art
Seth
Seunghee Han
Shahar Man
Shane McFly
Shawn Abelson
Shea Nangle
Shea Nangle
Shebin Mathew
SheHacksPurple
Shelly Giesbrecht
Shina Liu
Shir Sadon
Shishir Gupta
Shiva Shashank Kusuma
Shmuel Cohen
Shourya Pratap Singh
Shubham
Silvia Puglisi
Sim Cher Boon
Simone Stephen
SIV
Skittish and Bus
Soledad Antelada Toledano
Solomon Sonya
Soohwan Oh
Sorin Boloş
Spencer McIntyre
Spyros Gasteratos
Squiddy
Stephan Viljoen
Stephen Sims
Steve Dossey
Steve McGregory
Steven Sheffield
Sting
Stitcharoo
Stryker
Stryker
Stuart Wagner
Subho Majumdar
Sudhanshu
Sudipta Chattopadhyay
Suha Sabi Hussain
Suneel Sundar
Susan Greenhalgh
Susan Greenhalgh
Suzanne Borders
Sven Cattell
Sven Cattell
Sven Cattell
Sydney Johns

Sydney Johns
Sydney Marrone
Syed Aamiruddin
Syntax (DJ) + Luna (VJ)
Tailor Tolliver
Tal Folkman
Tal Folkman
Tal Folkman
Talk Sinn
Tarah Wheeler
Tarun Koyalwar
Ted Harrington
Tejas Patel
Tennisha Martin
Tennisha Martin
Terry Luan
th3CyF0x
The Glad Scientist
the gumshoo
The_Gibson
TheTechromancer
Thiago Bordini
Thiago Bordini
Thomas "Cr0wTom" Sermpinis
Thomas "Cr0wTom" Sermpinis
Thomas "stacksmashing" Roth
Thomas Boejstrup Johansen
Thomas Roccia
Thomas Roccia
Thomas X Meng
Tiernan "nvx" Messmer
Tim Chase
Tim Clevenger
Tim Clevenger
Tim Fowler
Tim Roberts
Timm Lauser
Tina Schneibs
Tina Velez
Todd Fletcher
Tom "Decius" Cross
Tom Boner
Tom Porter
Tom VanNorman
Tom VanNorman
Tomais Williamson
Tomer Peled
TommydCat
Tony Sager
Travis Weathers
Trey Bilbrey
Trey Bilbrey
TRIODE
Tristan Kalos
Troy Defty

Troy Defty
Trupti Shiralkar
TSA
TSA
TSA
TX
Tyler Casey
Ueric Melo
UK Repersentative 2
Utku Yildirim
Vadim Makarov
Vangelis Stykas
Vangelis Stykas
Varjitt Jeeva
Victor Fernandez Minguillon
Victor Pasknel
Victor Santos
Vikas Khanna
Viktor Gazdag
Vincent Lenders
Vincent Lenders
Vincent Sloan
Vinnie "kernelpaniek" Vanhoecke
Vinod Shrimali
Vishal Thakur
Vivek Ramachandran
Vivek Ramachandran
Vivek Ramachandran
Vivek Ramachandran
Vladyslav Zubkov
Vladyslav Zubkov
Wade Cappa
Walter J. Scheirer
Walter Scheirer
Wan Ding Yao
Wang Zhilong
WangJunJie Zhang
Wesley McGrew
Wesley McGrew
Wesley McGrew
WiGLE Staff
Will Baggett
Will Pearce
Will Pearce
William Loomis
William Phillips
William Taylor
Willis Vandevanter
Winson Tam
Woody
Wooseok Kim
Wouter Veenstra
Wyatt Ford
X
Xavier "rubix1138" Ashe

Xavier D. Johnson
Xavier Palmer
Xavier Zhang
Xiling Gong
Xinzhi Luo
xray
Xuan Xing
Yael Grauer
Yakir Kadkoda
Yan "Zardus" Shoshitaishvili
Yariv Tal
YiSheng He
Yisroel Mirsky
Yoann Dequeker
Yossi Pik
Yossi Pik
Yossi Pik
YTCracker
YTCracker
Yue Liu
Yurii Zadoianchuk
Zachary Stein
Zaire Moore
Zander Mackie
ZEE
Zibran Sayyed
Zoziel
ET E

Talk List

"BYOCTF" - Bring Your Own [Challenges||Capture] The Flag - BICV
(|(MaLDAPtive:¯_(LDAP)_/¯=ObFUsc8t10n) (De-Obfuscation &:=De*te)(!c=tion)) - DC
0.0.0.0 Day: Exploiting Localhost APIs From The Browser - APV
3D Printing My Way to Sanity: The Self-Funding Hobby That Changed Everything - MISC
3DU: Homo (e)x Machina - BHV
4G Frenzy - TCV
5G Fortress - TCV
5Ghoul Framework - 5G NR Attacks & 5G OTA Fuzzing - DL
A Bug Hunter's Guide to Account Takeover - BBV
A dive into world of Aircraft PKI - ASV
A Hacker's guide to PQC - QTV
A hole in one: pwning a cruise ship from a golf simulator and other tales of maritime IT-OT misconvergence - ICSV
A Reverse Engineer's Guide to AI Interpretability - AIxCC
A Shadow Librarian in Broad Daylight: Fighting back against ever encroaching capitalism - DC
A Short Introduction to 802.11ah Long Range WiFi HaLow with TaiXin TXW8301 devices - RFV
A Treasure Trove of Failures: What History’s Greatest Heist Can Teach Us About Defense In Depth - DC
A Whirlwind Tour of the FBI's Secret Encrypted Chat App - CPV
A Zero to Hero Crash Course to Server-Side Request Forgery (SSRF) - BBV
A-ISAC Aviation Cybersecurity Challenge - ASV
A-ISAC Aviation Cybersecurity Challenge - ASV
A-ISAC Aviation Cybersecurity Challenge - ASV
Abusando de Bitlocker para secuestrar información corporativa | Desde la intrusión hasta el descifrado (i) - MISC
Abusing DevOps to Pivot Between Cloud and On-Prem - RTV
Abusing legacy railroad signaling systems - DC
Abusing Windows Hello Without a Severed Hand - DC
Access Control Done Right the First Time - PSV
Access Control done right the first time - PSV
ACE up the Sleeve: From getting JTAG on the iPhone 15 to hacking into Apple's new USB-C Controller - DC
Activity: API Security 101: Testing and Trivia by Akto.io - APV
Activity: API Security 101: Testing and Trivia by Akto.io - APV
Activity: Capture the Container by Chainguard - APV
Activity: Capture the Container by Chainguard - APV
Activity: Hacking Developers’ Trust – Faking GitHub Contribution by Checkmarx - APV
Activity: Hacking Developers’ Trust – Faking GitHub Contribution by Checkmarx - APV
Activity: Spot the Reachable by Backslash - APV
Activity: Spot the Reachable by Backslash - APV
Activity: Spot the Reachable by Backslash - APV
Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - APV
Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - APV
Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian - APV
Activity: Test Your AppSec Knowledge by Deepfactor - APV
Activity: Threat modelling fun session with OWASP Cornucopia - APV
Activity: Threat modelling fun session with OWASP Cornucopia - APV
Activity: Vulnerability Hunt - The Snippets Edition - APV
Activity: Vulnerability Hunt - The Snippets Edition - APV
Advanced Packet Radio Operation - HRV
Adventures in Android Triage Collection - BTV
Adversarial AI: Disrupting Artificial Intelligence with Style - ADV
Adversary Simulation: Using Blue Eyes to See Red - RTV
Adversary simulator and purple teaming hands-on booth - ADV
Adversary simulator and purple teaming hands-on booth - ADV
Adversary simulator and purple teaming hands-on booth - ADV

Adversary Village keynote kick-off panel - ADV
Adversary-Adventure Table-top Game - ADV
Adversary-Adventure Table-top Game - ADV
Adversary-Adventure Table-top Game - ADV
Advocating for an Inclusive Cyber-Civil Rights Policy Agenda for Vulnerable Communities - PLV
AI Village Day 1 Keynote – Poison, injection, evasion, oh my! Grounding AI security threats in data driven reality - AIV
AI-Driven Cyber Resilience: Surviving the 5G Threat Landscape - TCV
AI'll be watching you. Greybox Attacks against an Embedded AI - AIV
Ain't that a Breach: Zero Trust Is the Only Solution! - BICV
AIxCC Closing Ceremonies - DC
All Your Keyboards Are Belong to US! - DC
AMA on Proxmark3 with Iceman - RFV
AMD Sinkclose: Universal Ring -2 Privilege Escalation - DC
Amenaza persistente: UXHIL y la propagación de URSA - MISC
An adversarial approach to Airline Revenue Management Proving Ground - ASV
An Operator's Guide: Hunting SCCM in the Real World - RTV
Analyzing the Security of Satellite-Based Air Traffic Control - ASV
Android App Usage and Cell Tower Location: Private. Sensitive. Available to Anyone? - DC
Anyone can hack IoT - a beginner's guide to hacking your first IoT device - IOTV
Application Threat Modeling with Trike - APV
AR + Art = interactive installations to bring your stories to life - XRV
Area DC32: An Interactive Tabletop Takes Flight (A BTV Panel) - BTV
ARINC 664 CTF - ASV
ARINC 664 CTF - ASV
ARINC 664 CTF - ASV
Arsenal: AI Goat - APV
Arsenal: CyberChef like Automation within BurpSuite - Let's get cooking with the CSTC - APV
Arsenal: GraphQL Armor - Open Source GraphQL Security - APV
Arsenal: HunterBounter - Swiss Army Knife for Bug Bounty - APV
Arsenal: Introducing RAVEN - Discovering and Analyzing CI/CD Vulnerabilities in Scale - APV
Arsenal: Kubescape - OSS security from left to right and everything in the middle - APV
Arsenal: SanicDNS - APV
Arsenal: SCAGoat - APV
Ask Me Anything - Daniel Cutberth, Moderated by Sudhanshu - RCV
Atomic Honeypot: A MySQL Honeypot That Drops Shells - DC
Attack and Defence in OT - Simulating attacks against hydroelectric power plants leveraging ICS Firing Ranges - ICSV
Attack Vectors of Quantum Computers - QTV
Attacking and defending card present transactions - PYV
Attacking and Defending Software Supply Chains: How we got Admin in your Clouds! - CLV
Attacks on GenAI data and using vector encryption to stop them - CPV
Automated Control Validation with Tommyknocker - DL
automobiles, alcohol, blood, sweat, and creative reversing of an obfuscated Car-Modding tool - DC
Aviation cybersecurity lightning talk: Three topics in thirty minutes - ASV
AWS CloudQuarry: Digging for secrets in public AMIs - DC
Badge Cloning: A Penetration Tester's Guide to Capturing and Writing Badges - RTV
Basic Mobile Phone Privacy - CPV
Basic Mobile Phone Privacy - CPV
Basic Packet Radio Operation - HRV
Bastardo Grande: Hunting the Largest Black Market Bike Fence In The World - RCV
Be Latino in Cybersecurity on markets outside LATAM - MISC
Be the Ghost in the Shell Barrier Mazes FTW - XRV
Behind Enemy Lines: Engaging and Disrupting Ransomware Web Panels - DC
Behind Enemy Lines: Going undercover to breach the LockBit Ransomware Operation - DC
Behind the Badge: How we used and abused hardware to create the AV badge for DC32 - ASV
Bespoke C2s are coming of age. - RTV

Beyond Sunset: Exposing the Occultations Lurking in Large-Scale Off-Grid Solar Systems - IOTV
BIC United Kingdom Chapter Informational Virtual Opening Session - BICV
BIC Village Keynote: Cyber Threat Landscape And Law Enforcement - BICV
BIC Village Opening Q&A with Marcus Hutchins - BICV
Blacks in Cyber Lituation 2.0 - SOC
Blue Goes Purple: Purple Teams for Fun and Profit (A BTV & RTV Panel) - RTV
Blue Team Careers: Do what you love, get paid for it! (A BTV Interactive Panel) - BTV
Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack - CHV
Bluetooth Landscape Exploration & Enumeration Platform (BLEEP) - DL
BOAZ, Yet Another layered Evasion Tool: Unveiling the Secrets Behind Antivirus Testing - RTV
Bogus Badges: The Art and Innovation of Badge Counterfeiting - PSV
BOLABuster: Harnessing LLMs for Automating BOLA Detection - AIV
BOLABuster: Harnessing LLMs for Automating BOLA Detection - APV
Book Signing: Visual Threat Intelligence: An Illustrated Guide for Threat Researchers - MISC
Breaching AWS Accounts Through Shadow Resources - DC
Breaking and Defending Cloud Infrastructure: Red Team Evasion Tactics and Access Control Solutions - DCGVR
Breaking Boundaries: Popping Shells in the Airgap with $10 and a Dash of Arduino Magic - BHV
Breaking Secure Web Gateways (SWG) for Fun and Profit - DC
Breaking software protected crypto implementations - PYV
Breaking the Beam: Exploiting VSAT Satellite Modems from the Earth's Surface - DC
Breaking Through Election Myths - VMV
Bricked & Abandoned: How To Keep The IoT From Becoming An Internet of Trash - DC
Bridging Space and Medicine - BHV
Bridging the Experience Gap in Machine Learning Security - AIV
Bridging the Gap: How the American Legion Provides Veterans with a Sense of Belonging and Support - MISC
Brief History of GRC - DCGVR
Bringing Down North Korea - DC
BTV Conversations: Exploring the Cyberpsychology of Cyber Defender Acceptance Behaviors and Personality Traits - BTV
BTV Conversations: Touch Grass to Combat Burnout - BTV
Building a Cyber Threat Intelligence Program from scratch for free! - BTV
Building a foundation with the 5 critical controls - ICSV
Building a secure and resilient nationwide EV charging network: the role of hackers in the clean energy revolution - CHV
Building Surgical Implants: A Comprehensive Guide to APT-style Techniques - RTV
Building the Ultimate Budget-Friendly Low Earth Orbit Satellite Ground Station - ASV
Building Your Red-Teaming Co-Pilot: Navigating the New Cyber Era with Pretrained Gen-AI - RTV
Building Zero Trust in ICS - ICSV
BYOS – Bring Your Own Satellite - ASV
Bypass 101 - PSV
Bypass 101 - PSV
Bypass 101 - PSV
Bypass 102 - PSV
Bypassing Corporate controls on Mac Devices - RTV
Bypassing WHOIS Rate Limiting and Alerting on Fresh Enterprise Domains - RCV
BypassIT - Using AutoIT & Similar Tools for Covert Payload Delivery - DL
Caido Internals Deep-Dive - BBV
Career Development - The Human Element - ICSV
Case Study: Hacking Smart Lock For Fun and Profit - MISC
Catch them all! Detection Engineering and Purple Teaming in the Cloud - CLV
Challenges and Reactions: Cybersecurity and Communications Resilience in Taiwan - PLV
Changing Global Threat Landscape with Rob Joyce and Dark Tangent - DC
Chatbots for Cybersecurity - MISC
Choose your own adventure: Has your fleet been hacked? - ASV
Clapping cheeks, aka home brew antennas - HRV
Clash, Burn, and Exploit: Manipulate Filters to Pwn kernelCTF - DC
Closing the Software Vulnerability Gap - AIxCC

Cloud Native Security Platform for Defenders - BTV
Cloud Offensive Breach and Risk Assessment (COBRA) - DL
Cloud Offensive Breach and Risk Assessment (COBRA) - CLV
Cloud Offensive Breaches: The Graph-Based Exploitation of Misconfigurations - RTV
Cloud Tripwires: fighting stealth with stealth - CLV
CODASM - Hiding Payloads in Plain .text - DL
Cognative Weather Report - VMV
Color Blasted Badge Making: How Hard Could It Be ? - MISC
Combining Uncensored and Censored LLMs for Ransomware Generation - RTV
Compromising an Electronic Logging Device and Creating a Truck2Truck Worm - DC
ConfusedPilot: Data Corruption and Leakage by Misusing Copilot for Microsoft 365 - AIV
Connecting the Dots: Mastering Alert Correlation for Proactive Defense in the Cloud - CLV
Contextualizing Open Source Software's Importance to CISA's Mission - AIxCC
CopyCat: An Artist Guide to Adversary Forgery - ADV
Correlating & contextualizing OT events/alerts/logs using weakly supervised AI - ICSV
Correlating slow & stealthy APT traces hiding in the sheer noise - ADV
Countdown to Industrial Extinction - ICSV
Covert Quantum Communication - QTV
Creating Azure Policy Compliant Backdoor - CLV
CTI is Dead, Long Live CTI: Reassessing Blue Team's Squishiest Value Proposition (BTV Panel) - BTV
CubeSat Simulator - ASV
CubeSat Simulator - ASV
CubeSat Simulator - ASV
CULT OF THE DEAD COW & Friends Present: Prime Cuts from Hacker History - 40 Years of 31337 - DC
Current EW techniques - RFV
Custom, cheap, easy, and safe badges - without starting from scratch - DC
Cyber Informed Engineering for Critical Infrastructure - ICSV
Cyber Security Transformation Chef (CSTC) - DL
Cyberjutsu Path to a Digital Martial Art - ADV
Cybersecurity for Emerging Tech (panelists would include researchers or industry executives in emerging tech categories, like space, OT, hardware like drones, etc) - MISC
Cybersecurity for Veterans: Bridging the Gap from Military to Civilian Careers - MISC
Cybersecurity Overview over LATAM- Skills, Challenges, Knowledge, Perspectives - MISC
Cybersecurity Schoolhouse Rock - PLV
D0N0H4RM: Cyber STEM Storytime - BHV
DarkGate: Cazando a la amenaza y exponiendo su infraestructura - MISC
Darkstar Badge Challenge - ASV
Darkstar Badge Challenge - ASV
Darkstar Badge Challenge - ASV
Data Brokers and the Threat to Your Privacy - CPV
Data On Demand: The challenges of building a privacy focused AI Device - CPV
DC NextGen / Youth Challenge Area at Red Team Village - RTV
DC NextGen / Youth Challenge Area at Red Team Village - RTV
DC NextGen / Youth Challenge Area at Red Team Village - RTV
DC101 Panel - DC
De Escudo a Espada: Cómo un Antivirus Facilitó el compromiso de una compañía - MISC
Deception & Counter Deception – Defending Yourself in a World Full of Lies - DC
Decoding Galah, an LLM Powered Web Honeypot - PHV
DEF CON Academy: Cultivating M4D SK1LLZ In the DEF CON Community - DC
DEF CON Closing Ceremonies & Awards - DC
DEF CON Franklin Project - DC
DEF CON Groups Panel #1 - DCGVR
DEF CON Unplugged: Cocktails & Cyber with Jeff & Jen - DC
Defeating EDR Evading Malware with Memory Forensics - DC
Defeating magic by magic Using ALPC security features to compromise RPC services - DC

Defend the Airport CTF - ASV
Defend the Airport CTF - ASV
Defend the Airport CTF - ASV
Democracy From Around the World - VMV
Detección de Vulnerabilidades mediante Instrumentación y su Explotación - MISC
Detect a Threat - ASV
Detect a Threat - ASV
Detect a Threat - ASV
Detouring Danger: Hunting Privileged File Operation Vulnerabilities in OT/ICS software - ICSV
Developing Better Payloads with Automated Testing - RTV
Developing Evilginx Phishlets - RTV
Differential privacy beyond algorithms: Challenges for successful deployment - CPV
Digital Emblems: When markings are required under international law, but you don’t have a rattle-can handy - DC
Discovering and exploiting local attacks against the 1Password MacOS desktop application - DC
Disenshittify or die! How hackers can seize the means of computation and build a new, good internet that is hardened against our asshole bosses' insatiable horniness for enshittification. - DC
distribRuted - Distributed Attack Framework - DL
Docker Exploitation Framework - DL
Does the World Need Another Threat Model, the Road to EMB3D - ICSV
DoH Deception: Evading ML-Based Tunnel Detection with Black-Box Attack Techniques - RTV
Don't Give Up The Ship! Maritime SOC/NOC Afloat - ICSV
Don't go too far… your job is not done! - MISC
Don't Ship Your Bridges! Tools to Explore Wireless Attack Surfaces in Every Ship's Marine Navigation Systems - ICSV
Doors, Cameras, & Mantraps: Oh my! - LPV
DoorSim - making my conference travel easier - RFV
Dragon SlayingGuide: Bug Hunting In VMware Device Virtualization - DC
DriverJack: Turning NTFS and Emulated Read-only Filesystems in an Infection and Persistence Vector - DC
Drone Capture the Flag (CTF) - ASV
Drone Capture the Flag (CTF) - ASV
Drone Capture the Flag (CTF) - ASV
Drone Flying Experience - ASV
Drone Flying Experience - ASV
Drone Flying Experience - ASV
Drone Hacking Activity - ASV
Drone Hacking Activity - ASV
Drone Hacking Activity - ASV
Drone Hacking Choose Your Own Adventure - ASV
Drone Hacking Choose Your Own Adventure - ASV
Drone Hacking Choose Your Own Adventure - ASV
Drop-Pi - DL
Dysfunctional Unity: The Road to Nowhere - BHV
Efficient Bug Bounty Automation Techniques - BBV
Election 2024 Freedom of Choice: A Psybernomic Conundrum - VMV
Emulating Magstripe with Arduino - PYV
Emulating Magstripe with Arduino - PYV
Encrypted newspaper ads in the 19th century - The world's first worldwide secure communication system - DC
Engineers & Exploits: The Quest for Security - APV
Epyon - Attacking DevOps environments - CLV
Eradicating Hepatitis C With BioTerrorism - DC
Eradicating Hepatitis C With BioTerrorism - BHV
Establishing the first Open Source Program Office at a United States Federal Agency - AIxCC
Evading Modern Defenses When Phishing with Pixels - ADV
Evaluations and Guardrails against Prompt Injection attacks on LLM powered-applications - AIV
Evolution of RF Signal Visualization - From Spectrum Analyzers to Augmented Reality - XRV
Expanding Pathways into the National Cyber Workforce - BICV

Exploit K8S via Misconfiguration .YAML in CSP environments - CLV
ExploitIfNotExists: Privilege Escalation & Persistence with Azure Policy - CLV
Exploiting Bluetooth - from your car to the bank account$$ - CHV
Exploiting Bluetooth - from your car to the bank account$$ - DC
Exploiting common vulnerabilities in AWS environments - CLV
Exploiting insecure OTA updates to create the worlds first Toothbrush Botnet and selfreplicating ESP32 worm - RFV
Exploiting the Unexploitable: Insights from the Kibana Bug Bounty - DC
Exploiting Voice Cloning in Adversarial Simulation - ADV
Exploration of Cellular Based IoT Technology - IOTV
Exploring Bias in AI-Assisted News - BICV
Exploring the Cosmos: Hackable Innovations at the Allen Telescope Array - RFV
Exposing Coordinated Attacks Hiding in the Sheer Noise of False Positives and Lone Incidents: A Data Science Correlation and Contextualization Journey of Logs, Events, and Alerts - PHV
Extend reality with tabletop RPG OWASP Cornucopia. Play sessions throughout workshop times. - XRV
FACTION - DL
Famous and Not-So-Famous Unsolved Codes - CPV
Farming Ndays with GreyNoise - DL
FIDO2 in the Quantum Realm - QTV
Finding 0days in Vilo Home Routers - IOTV
Finding Holes in Conditional Access Policies - CLV
Fine Grained Authorisation with Relationship-Based Access Control - APV
Fireside Chat with DNSA Anne Neuberger - DC
Fireside Chat with Jay Healey and National Cyber Director Harry Coker, Jr. - DC
First Time TSX Hacking Challenge - VMV
Fitness of Physical Red Teamers - PSV
Fix the Flag Wargame - APV
Fix the Flag Wargame - APV
Fix the Flag Wargame - APV
Flipping Locks (The Remix) - Remote Badge Cloning with the Flipper Zero and More - PSV
Flipping Locks (The Remix) - Remote Badge Cloning with the Flipper Zero and More - PSV
Fly Catcher - How I Developed a Low-Cost Raspberry Pi Based Device for ADS-B Spoof - ASV
Flying Blind: Navigating the Turbulent Skies of Aviation Cybersecurity Regulation - PLV
Fool us Once, fool us twice... Hacking Norwegian Banks - CPV
Forgetting the Fundamentals? Data Communications: Physical and Logical Explanation - ICSV
Formidable Adversaries: Responding to Breaches, Ransomware, and State-Sponsored Threat Actors - ADV
From CTI to Creating Campaigns - BTV
From Easy Wins to Epic Challenges: Bounty Hunter Edition - BBV
From Network to Network: Hands-On Pivoting Techniques in Internal Environments - RTV
From Redlining to Weblining: Examining Broadband Deserts and Racial Injustice - BICV
From research to release: Transferring AIxCC results to open source software - AIxCC
From Runners to IdP Admin - RTV
From Theory to Reality: Demonstrating the Simplicity of SPARTA Techniques - ASV
Front line first aid: Triaging your DFIR emergency responders - DCGVR
Fumbling into FedCyber - BICV
FuzzLLM: A Fuzzing Framework for Discovering Jailbreak Vulnerabilities in Large Language Models - BICV
garak : A Framework for Large Language Model Red Teaming - AIV
Garak - DL
GC2 - The First Serverless Command & Control - DL
GCPwn: A Pentester's GCP Tool - CLV
Generative AI vs Crusty NCO - MISC
Generative Red Team 2 Kickoff - AIV
Generative Red Team 2 Readout & Acknowledgements - AIV
GeoINT Mastery: A pixel is worth a thousand words - RCV
GHOST in the Model: Generating AI-Assisted Threat Models for Efficient Offensive Security Testing - RTV
Global Perspectives in Cybersecurity: Challenging Norms and Expanding Horizons - PLV

Gone in 60 Seconds… How Azure AD/Entra ID Tenants are Compromised - CLV
Gotta Cache ‘em all: bending the rules of web cache exploitation - DC
GPON Unplugged - TCV
GPS spoofing: it's about time, not just position - ASV
Grand Theft Actions: Abusing Self-Hosted GitHub Runners at Scale - DC
Gridlock: The Dual-Edged Sword of EV and Solar APIs in Grid Security - APV
Ground Control to Major Threat - Hacking the Space Link Extension Protocol - ASV
GUR RIBYHGVBA BS PELCGBTENCUL - CPV
Haciendo visible lo invisible: Observabilidad y transparencia en routers Draytek - MISC
Hack-A-Sat Digital Twin - ASV
Hack-A-Sat Digital Twin - ASV
Hack-A-Sat Digital Twin - ASV
Hack-A-Sat Quals Challenges - ASV
Hack-A-Sat Quals Challenges - ASV
Hack-A-Sat Quals Challenges - ASV
Hacker vs AI: perspectives from an ex-spy - PLV
Hacking Corporate Banking for Fun and Profit - APV
Hacking Millions of Modems (and Investigating Who Hacked My Modem) - DC
Hacking Policy and Policy Hacking - A Red-Teamer Hacker Guide to the Universe of Cyber Policy - RTV
Hacking Processes: Introducing the Redteaming Process Framework: RTPF - RTV
Hacking Quantum Key Distribution (QKD) - QTV
Hacking the Quansheng UV-K5 - HRV
Hacking the Skies – Satellite Red Teaming - RTV
Hacking the Vote: How Hackers Caused the Downfall of the Dutch Voting Machines - VMV
Ham in a Day Class - HRV
Ham Radio for Hackers - HRV
Ham Radio Fox Hunt - CON
Ham Radio Fox Hunt - CON
Ham Radio Fox Hunt - CON
Ham Radio in an HOA: Radio in the Face of Your Oppressor - HRV
HandPwning: "Your Hand is your Passport. Verify me. Now let me in!" - ICSV
HandPwning: “Your Hand is your Passport. Verify me. Now let me in!” - PSV
HandPwning: “Your Hand is your Passport. Verify me. Now let me in!” - PSV
Hands-on Attack and Breach Simulation exercises - ADV
Hands-on Attack and Breach Simulation exercises - ADV
Hands-on Attack and Breach Simulation exercises - ADV
Hands-On Container Image Security: Mastering Sigstore for Unbreachable Integrity - CLV
Hands-on Kubernetes security with KubeHound (purple teaming) - ADV
HDA Presents : Naomi Brockwell - HDA
HIDe & SEEK - DL
High Intensity Deconstruction: Chronicles of a Cryptographic Heist - DC
High ROI Manual Bug Hunting Techniques - BBV
HookChain: A new perspective for Bypassing EDR Solutions - DC
Hopper - Distributed Fuzzer - DL
Hospitals, Airports, and Telcos — Modern Approach to Attributing Hacktivism Attacks - RCV
Hot SOC Topics for 2024: Feel the Spice! - BTV
How can hackers support efforts to secure AI systems? - PLV
How Competitions Can Fuel Innovation - AIxCC
How do we make LLVM quantum? - QTV
How I discovered and hacked Learning Codes of the key job of a car assembled in my country - CHV
How I Learned to Stop Worrying and Love the Ban - DCGVR
How is GenIA Impacting Cybersecurity: The good, The Bad, and The ugly (Trilingual Panel) - MISC
How to Corrupt Youth to Cyber Focused Space Science - ASV
How to Find a 0day in iOS Apps - BICV
How to Steal Voting Software and Get Away With It - VMV

How we built our REDACTED THING this year, 5n4ck3y, && AMA Panel on Making Badges - MISC
Human Dignity in AI and Tech Policy - PLV
Hunters and Gatherers: A Deep Dive into the World of Bug Bounties - BBV
I am still the Captain now! - ICSV
I've got 99 problems but a prompt injection ain't pineapple - BBV
I've got 99 problems but a prompt injection ain't watermelon - APV
iCLASS - Throwing away the keys - RFV
Iconv, set the charset to RCE: exploiting the glibc to hack the PHP engine - DC
ICS 101 - ICSV
Identity Theft is not a Joke, Azure! - CLV
IDOR in Financial Operations - RTV
If Existing Cyber Vulnerabilities Magically Disappeared Overnight, What Would Be Next? - DC
Importance of ICS knowledge from a engineer's perspective - ICSV
Incident Response 101: Part 1 (IR Overview, Lifecycles, Frameworks, and Playbooks) - BTV
Incident Response 101: Part 2 (Analyst Mindset and Quality Assurance) - BTV
Incubated Machine Learning Exploits: Backdooring ML Pipelines Using Input-Handling Bugs - DC
Indivisible - VMV
Industry Panel: The Modern Evolution of LLMs - AIxCC
Injecting and Detecting Backdoors in Code Completion Models - APV
Insert coin: Hacking arcades for fun - RTV
Inside Dash Cam: Custom Protocols and Discovered 0-days - IOTV
Inside the FBI’s Secret Encrypted Phone Company ‘Anom’ - DC
Intermediate Physical Security - PSV
Interview - CATO Networks, Hosted by Dhruv Shah - RCV
Interview - Daniel Miessler, Hosted by Ankur - RCV
Interview - Mika Devonshire, Hosted by Himanshu Das - RCV
Interview - RedHunt Labs (Kunal), Hosted by Anant Shrivastava - RCV
Interview - Scott Helme, Hosted by Shubham - RCV
Interview - the gumshoo, Hosted by Ram - RCV
Intro to QKD: Quantum Key Exchange: Beyond the Hype - QTV
Intro to Quantum with Q# - QTV
Introduction to Creating Osquery Extensions: Enhancing Endpoint Security Visibility - BTV
Introduction to Drone Security - ASV
Introduction to IPv6 - PHV
Introduction to Kubernetes common attack techniques - RTV
Introduction to MITRE Caldera Through Adversary Emulation - ADV
Introduction to Payment Village CTF - PYV
Introduction to Payment Village CTF - PYV
Introduction to the Payment Village badge - PYV
Invisible Invaders: Strategies to Combat Living Off the Land Techniques in ICS - ICSV
IoT Cat Lamp - IOTV
IoT Cat Lamp - IOTV
Island Hoping: Move from LOLBins to Living off Langs - RTV
Jack Rhysider Masquerade Party - SOC
Jayson Street - Keynote - DCGVR
Jayson Street - Keynote - DCGVR
Jeitinho Cibernético: A Convergência da Segurança no Brasil e América Latina - MISC
Joe and Bruno's Guide to Hacking Time: Regenerating Passwords from RoboForm's Password Generator - DC
Keynote - AI-Powered Cybersecurity: The Importance of Red Teamers - AIV
Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access - CLV
Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access - DC
Kubernetes Attack Simulation: The Definitive Guide - ADV
Kubernetes Security: Hands-On Attack and Defense - APV
Laundering Money - DC
Learn BadUSB Hacking With the USB Nugget - IOTV

Learn Beginner Soldering With the Meow Mixer Badge - IOTV
Learning the New Amass Collection Engine - RTV
Level UP OSINT - RTV
Leveraging AI for Smarter Bug Bounties - BBV
Leveraging Internal Systems for Enhanced Bug Bounty Success - BBV
Leveraging private APNs for mobile network traffic analysis - DC
LFG! Forming a Bug Bounty Hunting Party - BBV
Life, Liberty and the pursuit of Convenience: the slow death of independence - BICV
Listen to the whispers: web timing attacks that actually work - DC
Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - IOTV
Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - IOTV
Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers - IOTV
Locksport Competitions: Compete in the Olympics of Locks - LPV
LoRa for Hackers : Long Range Hacking for Beginners With CircuitPython - IOTV
Lost in Translation - WAF Bypasses By Abusing Data Manipulation Processes - BBV
Low Power & Long Range Communications - QRP - HRV
Mac-n-Cheese: How to Cook Up Delicious Electron Techniques for Red Teamers - RTV
macOS Red Team on Corporate Scenarios - RTV
Maestro - DL
Make all the things - Construa seus próprios "brinquedos" Threats - MISC
Making the DEF CON 32 Badge - DC
Maltego Community Workshop - RCV
Manufacturing- Lessons Learned, Lessons Taught - ICSV
Mapping the Landscape: Top 10 Cybersecurity Trends in Critical Infrastructure for 2024 - ICSV
Maricopa County -Preparing for the 2024 Elections Cycle - VMV
Master Splinter’s initial physical access dojo: Storytelling of a complex adversarial attack - ADV
Maturing Your Application Security Program - APV
MCPA x BIC x CAPT Virtual National Service Panel 2024 - BICV
Measuring the international balance of trade in Internet bandwidth: introducing Netflow to Ministries of Finance - PLV
Measuring the Tor Network - DC
Meet the PortSwigger Research team (Q/A) - BBV
Meshtastic Adventures: Triumphs, Tribulations, and Total Mesh-ups. - RFV
Meshtastic Meetup - IOTV
Meshtastic Meetup - IOTV
Mexicans Together - Un vistazo a recientes investigaciones de nuestros dos equipos globales - MISC
MFT: Malicious Fungible Tokens - ADV
Microhard? More like MicroEASY...to exploit... - IOTV
Mind-Controlling Other Applications: An intro to intra-process hacking - APV
Mining for Abandoned Gold in DNS - RTV
Misinformation, Disinformation, and Malformation in 2024 - VMV
MITRE Caldera for OT - DL
MITRE Caldera - DL
Mobile Mesh RF Network Exploitation: Getting the Tea from goTenna - DC
Modern Red Teaming: macOS, K8s, and Cloud - RTV
Modifying Impacket for Better OpSec - RTV
Modifying Impacket for Better OpSec - ADV
Moriarty - DL
MoWireless MoProblems: Modular Wireless Survey Systems and the Data Analytics That Love Them - PHV
MPT - Pentest in Action - DL
Music Set / Entertainment (Cyberpunk Bar Friday, ACK Stage) - SOC
Music Set / Entertainment (Cyberpunk Bar Saturday, ACK Stage) - SOC
Music Set / Entertainment (Cyberpunk Bar Thursday, ACK Stage) - SOC
Music Set / Entertainment (Pirate's Night For Me! Saturday, SYN Stage) - SOC
Music Set / Entertainment (Retro Sci-Fi Friday, SYN Stage) - SOC
Music Set / Entertainment (Thursday, SYN Stage) - SOC

Mutual authentication is optional - DC
My Conversations with a GenAI-Powered Virtual Kidnapper - AIV
My Smart Red Team Copilot - BICV
Nano-Enigma: Uncovering the Secrets Within eFuse Memories - DC
National Labs Use of XR - XRV
Navigating Bureaucracy: Strategies for a Post-Military Career Encore - MISC
Navigating Microaggressions and Fostering Inclusive Communication with Peers and Leadership for Black Professionals - BICV
Navigating the Cyber Security Labyrinth: Choose Your Own Security Adventure? - APV
Nebula - 3 Years of Kicking *aaS and Taking Usernames - DL
New Skill Unlocked: C2 Infrastructure Automation - RTV
No CTF? No Problem! Leveraging Alternate Reality Games to Develop OSINT and Cryptography Skills - MISC
No Symbols When Reversing? No Problem: Bring Your Own - DC
No Time for Complacency: The Stakes of AI in Cybersecurity - AIxCC
NSM-22 and the National Risk Management Plan: CISA Wants to Hear from You on How to Protect Our Nation's Critical Infrastructure - PLV
NTLM - The Last Ride - DC
Obsidian: Forensics 101 Part 1 - BTV
Obsidian: Forensics 101 Part 2 - BTV
Offensive Security Testing: Safeguarding the Final Frontier - ASV
OH-MY-DC: Abusing OIDC all the way to your cloud - DC
On Your Ocean's 11 Team, I'm the AI Guy (technically Girl) - DC
On Your Ocean's 11 Team, I'm the AI Guy (technically Girl) - AIV
One Click, Six Services: Abusing The Dangerous Multi-service Orchestration Pattern - CLV
One for all and all for WHAD: wireless shenanigans made easy ! - DC
One Port to Serve Them All - Google GCP Cloud Shell Abuse - CLV
Online Payments - Attack and Defense - PYV
Open Hardware Design for BusKill Cord - DL
Open sesame - or how vulnerable is your stuff in electronic lockers - DC
Open Source Drone Hacking Simulator - ASV
Open Source Hacker Vs. Government Lawyer: Clashing Views on Fixing Tech in the DoD - PLV
Opening Remarks - AIV
Optical Espionage: Using Lasers to Hear Keystrokes Through Glass Windows - DC
OSINT at Clemson: Unmasking John Mark Dougan's Disinformation Empire - RCV
OSINT for Hackers - RTV
OT Incident response and Threat Hunting - ICSV
Outlook Unleashing RCE Chaos: CVE-2024-30103 & CVE-2024-38021 - DC
OWASP Amass Expanding Data Horizons: Amassing More Than Subdomains - RCV
Panel of Bug Bounty Community Leaders - BBV
Photoshop Fantasies - AIV
Physical Fundamentals of Quantum Computing - QTV
Physical OSINT - PSV
Physical Red Teaming for Offensive Cyber Teams - RTV
Physical Security - Bypassing Access Control Systems - RTV
Physical Security Assessment Basics for Internal Employees - PSV
Pick Your Poison: Navigating a secure clean energy transition - PLV
Pipeline Pandemonium: How to Hijack the Cloud and Make it Rain - RTV
Play by Play of the Curling v. Raffensperger Lawsuit - VMV
Playing with Quantum: wayfinding with quantum game theory - QTV
Porn & Privacy - CPV
Power To The Purple - ADV
Practical Exploitation of DoS in Bug Bounty - BBV
Prendendo Fraudadores utilizando Técnicas de Red Team - MISC
Preparing for the Future: A Discussion of our Rapidly Evolving Threat Landscape - IOTV
Product security considerations for OT security appliances - ICSV

Programming a CTS-V Gauge Cluster into an ATS-V, out of pure spite - CHV
Protecting the Backbone of Our Modern World - MISC
Prototype Pollution in Depth, From Beginner to 0-Day Hunter - BBV
Psychic Paper: Making eink access badges accessible for anyone - IOTV
PTP Flight Challenge - ASV
PTP Flight Challenge - ASV
PTP Flight Challenge - ASV
Pushing the limits of mass DNS scanning - RCV
Pwning through the Metaverse - Quest Headset Vulnerability Research - XRV
QML - Quantum Machine Learning: What is it, where did it come from, and how do I start? - QTV
Quantum on the flip side - A global south perspective on Quantum Technologies - QTV
QuickShell: Sharing is caring about an RCE attack chain on Quick Share - DC
Ransomware B-Sides: Los ransoms que nunca triunfaron - MISC
Recon MindMap: Organize, Visualize, and Prioritize Your Recon Data Efficiently - RCV
Recursion is a Harsh Mistress: How (Not) To Build a Recursive Internet Scanner - RCV
Red Goes Purple: Executing the Attack Path - RTV
Red Team Infrastructure Setup and Automation - RTV
Red Team Terraform Workshop - RTV
Red Teaming is broken; this panel will fix it. - ADV
Redefining V2G - How to use your vehicle as a game controller - DC
Reflections on a Decade in Bug Bounties: Experiences and Major Takeaways - BBV
Relative Path File Injection: The Next Evolution in RPO - APV
Remote Sensor Node Updates for FISSURE - The RF Framework - RFV
Removing OPSEC from Cyber Predators and Threat Actors - MISC
Removing the Ring of Gyges: Lessons from Securing AI Systems Against File Format Abuse - AIV
Revealing Choke Points: Practical Tactics for Boosting Cloud Security - CLV
Reverse engineering and hacking Ecovacs robots - ESV
Reverse Engineering MicroPython Frozen Modules: Data Structures, Reconstruction, and Reading Bytecode - DC
RF Attacks on Aviation's Last Line of Defense Against Mid-Air Collisions (TCAS II) - ASV
RF CTF Kick Off Day 1 - RFV
RF CTF Kick Off Day 2 - RFV
RFID 101 - PSV
Risk Limiting Audit DEMO by Philip Stark - VMV
Risk Limiting Audits From the Source - VMV
Rules All Hackers Must Follow in War - PLV
Runtime Reachability: Prioritizing Vulnerabilities with eBPF & Continuous Profiling - CLV
RustOps - RTV
Safecracking for Everyone - LPV
Safecracking Practical Demonstration - LPV
SBOMs the Hard Way: Hacking Bob the Minion - IOTV
SCAGoat - Exploiting Damn Vulnerable SCA Application - DL
SDLC Nightmares - Defeating Secure Code Review GPT Hallucinations - APV
Secrets and Shadows: Leveraging Big Data for Vulnerability Discovery at Scale - DC
Secure the Skies: A Modern Android Security Research Framework for Drone Ground Control Stations and Applications - ASV
Securing CCTV Cameras Against Blind Spots - DC
Securing Frontends at Scale: Paving our Way to the Post-XSS World - APV
Securing Health Care: AIxCC, DIGIHEALS, and UPGRADE - AIxCC
Securing the Cloud with Cloud Threat Intelligence and Open Source Security - BTV
Securing the Future with CoSAI: Identified Technical Workstreams and Call for Contributions - RTV
Securing the Harvest: Cyber Defense for Agricultural Control Systems - ICSV
Seeing the Unseen: An Evaluation of Active Scanning in ICS Environments - ICSV
Selfie with a CubeSat - ASV
Selfie with a CubeSat - ASV
Selfie with a CubeSat - ASV

Serberus - DL
Shifting left in Reversing apk by converting smali to java - DCGVR
SHIM me what you got - Manipulating Shim and Office for Code Injection - DC
Signature-Based Detection Using Network Timing - PHV
SIMply Secure - TCV
Simulated Drone Hacking - RTV
Singapore - Safeguarding the Nation: The Vital Role of Cybersecurity in AI-Driven Homeland Security - PLV
SIV Internet Voting Hacking Challenge - VMV
Skynet - DL
Small Satellite Modeling and Defender Software - ASV
Smart Shopping Cart Wheels - How they Work - PSV
Smishing Smackdown: Unraveling the Threads of USPS Smishing and Fighting Back - DC
SMOKE: Signature Management using Operational Knowledge and Environments - AIxCC
Sneaky Extensions: The MV3 Escape Artists - ADV
So you wanna know how to make badges - MISC
Social Engineering Improv Acting Techniques - PSV
Social Engineering Like you're Picard - DC
Software Defined Radio 101: Capturing Your First RFCTF Flag - RFV
Sold Out - 64-bit Intel Assembly Language Programming for Hackers - WS
Sold Out - Capture the Flag 101 - WS
Sold Out - Crash Course in Physical Access Control Systems - WS
Sold Out - Dissecting and Defeating Ransomware's Evasion Tactics - WS
Sold Out - Dissecting Malware for Defense - Crafting Custom Yara Rules - WS
Sold Out - Dodging the EDR Bullet: A Workshop on Malware Stealth Tactics - WS
Sold Out - Email Detection Engineering and Threat Hunting - WS
Sold Out - Finding the Needle: An Introduction to Detection Engineering - WS
Sold Out - Flipping the Coin: Red and Blue Teaming in Windows Environments (++) - WS
Sold Out - From an attacker's lair to your home: A practical journey through the world of Malware - WS
Sold Out - Ghidra Analysis & Automation Masterclass - WS
Sold Out - Hack the connected plant! - WS
Sold Out - Hacking Apps on Salesforce - WS
Sold Out - Hacking The Metal: A Spark of Intelligence - WS
Sold Out - Hide your kids, turn off your Wi-Fi, they Rogue APing up in here; 201 - WS
Sold Out - Industrial Control Systems: how to secure them in practice! - WS
Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF - WS
Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming - WS
Sold Out - Machine Learning for N00bs - WS
Sold Out - Master Class: Hands-On Machine Learning to Enhance Malware Analysis, Classification, and Detection - WS
Sold Out - Med Team vs Red Team: Intro into Medical Device Hacking - WS
Sold Out - Offensive SCCM: Abusing Microsoft's C2 Framework - WS
Sold Out - Playing with RFID - WS
Sold Out - Sharp Security from All Angles: Mastering Security in .NET Core 8 and Angular 17 Applications - WS
Sold Out - Small Choices, Global Repercussions: A Tabletop Exercise about Decision-Making in Healthcare Cybersecurity - WS
Sold Out - Supercharge SAST: Semgrep Strategies for Secure Software - WS
Sold Out - Tracing The Pain Away - Practical Binary Tracing Techniques For Defeating Modern Malware Protections - WS
Sold Out - Traumatic Library Loading : If you want to use it, you have to implement it... - WS
Sold Out - Whitebox Web Exploit Development - WS
Solder your own cat shaped WiFi Haking tool - IOTV
Solving the "Lover, Stalker, Killer" Murder with strings, grep, and Perl - DC
Something something Meshtastic Pip-Boy Personal Mesh with 150 km reach - DCGVR
Space Grand Challenge Luna - ASV
Space Grand Challenge Luna - ASV
Space Grand Challenge Luna - ASV
Space Pirate Simulator - ASV

Space Systems Security CTF – Platform Security - ASV
Space Systems Security CTF – Platform Security - ASV
Space Systems Security CTF – Platform Security - ASV
spacestudio and spacetower challenges - ASV
spacestudio and spacetower challenges - ASV
spacestudio and spacetower challenges - ASV
Speed Bumps and Speed Hacks: Adventures in Car Manufacturers Security - APV
Spies and Bytes: Victory in the Digital Age - DC
Splitting the email atom: exploiting parsers to bypass access controls - DC
Spotting Deepfakes in a World with Generative AI - AIxCC
SQL Injection Isn't Dead: Smuggling Queries at the Protocol Level - DC
SQLi to Root Access: Exploiting a ISP infrastructure - MISC
Sshamble: Unexpected Exposures in the Secure Shell - DC
SSTV: How To Send Cat Memes Via Ham Radio - HRV
Stanford Digital Observatory - VMV
Staying alive off the grid - using APRS and Lambdas to monitor temperature remotely - HRV
Stealer Logs: Automation, Analysis, & Espionage in the World's Most Interesting Dataset - BTV
Store bought is fine, sometimes! - BTV
Stranger in a Changed Land - DC
Structural Insights: PDF Analysis for Detecting and Defending Against Threats - MISC
Student Engagement Doesn't Have to Suck - XRV
Sudos and Sudon’ts - Peering inside Sudo for Windows - DC
Supercharge your vuln finding workflow with automated labs: How Ludus made it rain creds from SCCM - RTV
Surprise Talk - CPV
SWGRecon: Automate SWG Rules, Policy, and Bypass Enumeration - RCV
Taking off the blindfold: Detecting persistent threats on Draytek edge devices - DC
Taming the Beast: Inside the Llama 3 Red Team Process - DC
Tapping the OSINT potential of Telegram - RCV
Techniques for Creating Process Injection Attacks with Advanced Return-Oriented Programming - DC
Telecom Time Machine - TCV
Tempest c2: Use and Design - RTV
Tempest - DL
Tengu Marauder - DL
Terraform Unleashed: Crafting Custom Provider Exploits for Ultimate Control - CLV
Testbed Virtual Factory - DL
The Art of Critical Thinking through an Adversarial Mindset? (RTV Keynote) - RTV
The art of Pivoting in OSINT Investigations - RCV
The Bug Hunters Methodology Live - DEF CON Edition - BBV
The Cat-and-Mouse Game of Adversarial Artificial Intelligence - AIxCC
The Curious Case of Alice and Bob: What You Can (And Cannot!) Do as Digital Investigators - PHV
The Curious Case of Stealer Logs: Access & Espionage in the World's Most Interesting Dataset - RTV
The Dark Side of Bug Bounty - APV
The hack, the crash and two smoking barrels. (And all the times I (almost) killed an engineer.) - DC
The Hybrid Horizon: Unleashing the Power of Azure Hybrid Integrations - RTV
The Immortal Retrofuturism of Mainframe Computers and How to Keep Them Safe - APV
The Implications of Cyberbiosecurity in Advanced Agricultural Systems - BICV
The Interplay between Safety and Security in Aviation Systems - ASV
The Metasploit Framework v6.4 - DL
The Missing Link - How we collect and leverage SBOMs - APV
The not-so-silent type: Breaking network crypto in almost every popular Chinese keyboard app - DC
The Open Source Fortress: Finding Vulnerabilities in Your Codebase Using Open Source Tools - APV
The Oracle Awakens: Demystifying Privilege Escalation in the cloud - CLV
The Past, Present, and Future of Bioweapons - BHV
The People's Republic of Fieldbus: What to know about EPA - ICSV
The perma-lag: why industrial cybersecurity will never be state-of-the-art - ICSV

The Quantum Ethics and Skills Debates - QTV
The Rise and Fall of Binary Exploitation - DC
The Rise of the Planet of the Agents: LLM-based AI Agents and Cloud Security APIs - CLV
The Risk and Reward of Distributed Industrial Control - ICSV
The Sand Castle - The State of the MacOS Sandbox - DCGVR
The Secret Life of a Rogue Device - Lost IT Assets on the Public Marketplace - DC
The SIEMless Hack: Rewriting Reality with Log Injection - RTV
The Threat of Deepfakes and Synthetic Media to Election Integrity - VMV
The Transparency Algorithm: AI's Answer to Legal Racial and Social Inequality - BICV
The Value of Trust in the Open-source Software Ecosystem - PLV
The Village Peoples' Panel - What Really Goes On in a Village? - RTV
The Way To Android Root: Exploiting Your GPU On Smartphone - DC
The wild and wonderful world of early Microprocessors (with a focus on the 6502) - DC
The World Wide Paraweb - DL
The XZ Backdoor Story: The Undercover Operation That Set the Internet on Fire - DC
TheAllCommander 2.0 - DL
Thinking Outside the Kube - Finding and Exploiting Command Injections in Kubernetes - RTV
Threat Emulation 101 - RTV
Threat Hunting + Intelligence, capabilities, skills and capabilities inside the LATAM community - MISC
Threat hunting like a pentester - RTV
Threat Modeling in the Age of AI - APV
Threats in Space: The Dangerous Rise of GNSS Attacks - MISC
Thrunting or DEATH! (A BTV Panel) - BTV
Ticking SQLi - APV
Top War Stories from a TryHard Bug Bounty Hunter - BBV
Tough Adversary? Don’t Blame Sun Tzu - ADV
Tracking Industrial Advanced Threat Actors Who Aren't Really Advanced Just Skiddies Who Deface PLCs and Have Bad Manners: Methods and Results - ICSV
Tracking Real-Time Locations with Rogue WiFi Packets - RFV
Transforming AppSec: Protecting 'Everything as Code' & Emerging Tech - APV
Trapped Ion Quantum Computing Systems - Behind The Scenes: from the physics to control electronics - QTV
Travel Better: Expedient Digital Defense - CPV
Trip Through Reality XR for Performances Masterclass with the Glad Scientist - XRV
Troll Trapping Through TAS Tools - Exposing Speedrunning Cheaters - DC
Tunnel Vision: Exploring VPN Post-Exploitation Techniques - RTV
UDSonCAN Attacks: Discovering Safety-Critical Risks by Fuzzing - CHV
Under the Hood: Incident Response at High Speed (A BTV Panel) - BTV
Understanding Cognitive Warefare in a Geopolitcal Context - VMV
Understanding the Role of Secretary of States in Elections - VMV
Underway to Identifying Commonalities of Cybersecurity Incidents in the Maritime Transportation System - ICSV
Unexpected Leaks in AWS Transit Gateways - CLV
Unlocking Hidden Superpowers: Neurodiversity in Infosec - DCGVR
Unlocking the Gates - Understanding Authentication Bypass Vulnerabilities - APV
Unlocking the Gates: Hacking a secure Industrial Remote Access Solution - DC
Unmasking Shadows: Strategies on Hunting Ransomware Groups - BICV
UnOAuthorized: Discovering the path to privilege elevation to Global Administrator - CLV
Unsaflok: Hacking millions of hotel locks - DC
Unveiling Vulnerabilities: A Comprehensive Guide to Bug Bounty Recon - BBV
US and International Public Cyber Policy 101 - PLV
Use opensource AI to map alerts & logs into techniques, clusters, and killchains - BTV
User Behaviour Analytics in Payments - PYV
Using AI Computer Vision in Your OSINT Data Analysis - PHV
Using ChatGPT to Write Defensive & Offensive Tools for ICS/OT - ICSV
Using EPSS for Better Vulnerability Management - APV
Using Retrieval Augmented Generation (RAG), Langchain, and LLMs for Cybersecurity Operations - RTV

V2GEvil: Ghost in the wires - CHV
Veilid Dev and Community Meetup - DC
Village closing - ADV
Virtual SIEM/SOAR Workshop - BICV
Visualizing AIxCC: Bringing Your Code to Life - AIxCC
Volatile Vault - Data Exfiltration in 2024 - DL
Voting Village Opening Remarks - VMV
Vovk - Advanced YARA Rule Generator v2.0 - DL
War Games: Red Team for OT (Based on Real World Case Studies) - ICSV
Warflying in a Cessna - ASV
Warwheeling: The Wireless Sk8r - RFV
Watch The Skies: Build Your Own ADS-B receiver - ASV
Watchers being watched: Exploiting the Surveillance System and its supply chain - DC
Weaponized Convenience: Inside the Rise of Remote Tool Abuse - BICV
Web2 Meets Web3: Hacking Decentralized Applications - APV
Welcome to DEF CON - DC
What Do Long Voter Registration Lines Mean? - VMV
What Does it Mean to be an American? - VMV
What is the Voting Village? - VMV
What To Expect When You're Exploiting: Attacking and Discovering Zero-Days in Baby Monitors and Wi-Fi Cameras - IOTV
What!? Is my life that fragile? - DCGVR
What's next for the commercial CNE marketplace? A chance for you to influence the policy that will impact the future - PLV
When Chatbots Go Rogue – Lessons Learned from Building and Defending LLM Applications - APV
Where's Waldo? Can you find the Raspberry Pi in the Cyber Defense Exercise? - ICSV
Where's the Money: Defeating ATM Disk Encryption - IOTV
Where's the Money: Defeating ATM Disk Encryption - DC
Who cashed my check?! Catching (Very Obvious) Fraudsters - DCGVR
Who's Afraid of Synthetic Aperture Radar? - RFV
Why are you still, using my server for your internet access. - DC
Why You Should Be Hunting on Web3 Bug Bounties - BBV
Wi-Fi Hacker Hunting - IOTV
Wi-Fi Hacking Self Defense: Four Advanced Techniques and How to Stop Them - IOTV
Windows Downdate: Downgrade Attacks Using Windows Updates - DC
Winning big: AppSec Considerations From the Casino Industry - APV
Winning the Game of Active Directory - PHV
Wireless & Networking workshop - ESV
Wireless & Networking workshop - ESV
Wireless & Networking workshop - ESV
World Wide War Drive Outbrief - RFV
Worried about AI taking your job? Then this talk is for you. - BICV
Wu-Tang is for the Children: How States Laws Intended to Protect Children Raise Other Privacy and Legal Risks - CPV
XenoboxX - Hardware Sandbox Toolkit - DL
Xiaomi The Money - Our Toronto Pwn2Own Exploit and Behind The Scenes Story - DC
XR for All: Accessibility and Privacy for Disabled Users - XRV
Yet another way of exfiltrating data from air-gapped systems OR Oh no, everything is a radio - RFV
You got a lighter? I need to do some Electroporation. - BHV
Your AI Assistant has a Big Mouth: A New Side-Channel Attack - DC
Your CI/CD Pipeline Is Vulnerable, But It's Not Your Fault - APV
Your Smartcard is Dumb: A Brief History of Hacking Access Control Systems - PSV
Zip It Up, Sneak It In - Introduction of apkInspector - DL

Village Talk List

ADV - Adversary Village

Location: LVCC West/Floor 1/Hall 4/HW4-03-05 - Map
Home Page: https://adversaryvillage.org
Sched Page: https://adversaryvillage.org/adversary-events/DEFCON-32/

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Hands-on Attack and Breach Simulation exercises	Adversary Village Crew
10:00 - 17:59	Adversary simulator and purple teaming hands-on bo . . .	Adversary Village Crew
10:00 - 17:59	Adversary-Adventure Table-top Game	Adversary Village Crew
10:00 - 10:59	Adversary Village keynote kick-off panel	Abhijith “Abx” B R,Br . . .
11:30 - 12:30	Formidable Adversaries: Responding to Breaches, Ra . . .	Abhijith “Abx” B R,Ad . . .
11:00 - 12:59	Modifying Impacket for Better OpSec	Ryan O'Donnell
12:30 - 12:59	MFT: Malicious Fungible Tokens	Cybelle Oliveira ,Mauro E . . .
13:00 - 14:59	Introduction to MITRE Caldera Through Adversary Em . . .	Rachel Murphy,Mark Perry
15:00 - 16:59	Hands-on workshop	
16:30 - 16:59	Master Splinter’s initial physical access dojo: . . .	Daniel Isler
17:00 - 17:59	Red Teaming is broken; this panel will fix it.	Suneel Sundar,Niru Ragupa . . .
Saturday		
10:00 - 10:30	Sneaky Extensions: The MV3 Escape Artists	Vivek Ramachandran,Shoury . . .
10:30 - 10:59	Tough Adversary? Don’t Blame Sun Tzu	Gregory Carpenter
10:00 - 17:59	Adversary-Adventure Table-top Game	Adversary Village Crew
10:00 - 17:59	Hands-on Attack and Breach Simulation exercises	Adversary Village Crew
10:00 - 17:59	Adversary simulator and purple teaming hands-on bo . . .	Adversary Village Crew
10:00 - 10:59	Adversarial AI: Disrupting Artificial Intelligence . . .	Chloé Messdaghi,Sebastia . . .
11:00 - 11:30	Evading Modern Defenses When Phishing with Pixels	Melvin Langvik
11:00 - 11:59	Power To The Purple	Tyler Casey,Trey Bilbrey
12:00 - 13:59	Hands-on Kubernetes security with KubeHound (purpl . . .	Julien Terriac
14:00 - 15:59	CopyCat: An Artist Guide to Adversary Forgery	Cat Self
16:00 - 17:59	Cyberjutsu Path to a Digital Martial Art	Alexandre CABROL PERALES, . . .
Sunday		
10:00 - 11:59	Adversary-Adventure Table-top Game	Adversary Village Crew
10:00 - 11:59	Hands-on Attack and Breach Simulation exercises	Adversary Village Crew
10:00 - 11:59	Correlating slow & stealthy APT traces hiding in t . . .	Ezz Tahoun
10:00 - 11:59	Adversary simulator and purple teaming hands-on bo . . .	Adversary Village Crew
11:30 - 11:59	Kubernetes Attack Simulation: The Definitive Guide	Leo Tsaousis
11:00 - 11:30	Exploiting Voice Cloning in Adversarial Simulation	Mark Foudy
12:00 - 12:59	Village closing	Adversary Village Crew

Return to Index

AIV - Artificial Intelligence Village

Location: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map
Home Page: https://aivillage.org/
Sched Page: https://aivillage.org/events/
DC Discord Chan: https://discord.com/channels/708208267699945503/732733090568339536

PDT Times	Title	speaker
Friday		
10:30 - 11:30	Generative Red Team 2 Kickoff	Sven Cattell,Will Pearce, . . .
10:00 - 10:30	Opening Remarks	Sven Cattell,Lauren Putvi . . .
10:00 - 17:59	AI Village Demos	
11:30 - 12:30	BOLABuster: Harnessing LLMs for Automating BOLA De . . .	Ravid Mazon,Jay Chen
13:30 - 14:30	AI'll be watching you. Greybox Attacks against a . . .	Ryan Tracey,Kasimir Schul . . .
14:30 - 14:59	Removing the Ring of Gyges: Lessons from Securing . . .	Sean Oesch,Luke Koch,Bria . . .
15:00 - 15:59	On Your Ocean's 11 Team, I'm the AI Guy (techn . . .	Harriet Farlow
16:00 - 16:59	AI Village Day 1 Keynote – Poison, injection, ev . . .	Christina Liaghati
Saturday		
10:00 - 10:59	Keynote - AI-Powered Cybersecurity: The Importance . . .	Nikki Pope
10:00 - 17:59	AI Village Demos	
11:30 - 12:30	garak : A Framework for Large Language Model Red T . . .	Leon Derczynski,Erick Gal . . .
13:30 - 14:30	ConfusedPilot: Data Corruption and Leakage by Misu . . .	Ayush RoyChowdhury,Mulong . . .
14:30 - 14:59	Evaluations and Guardrails against Prompt Injectio . . .	Cyrus Nikolaidis,Faizan A . . .
15:00 - 15:59	Bridging the Experience Gap in Machine Learning Se . . .	Kellee Wicker (Moderator) . . .
Sunday		
10:00 - 10:59	Photoshop Fantasies	Walter Scheirer
10:00 - 12:59	AI Village Demos	
11:00 - 11:30	My Conversations with a GenAI-Powered Virtual Kidn . . .	Perry Carpenter
12:00 - 12:59	Generative Red Team 2 Readout & Acknowledgements	Sven Cattell,Will Pearce, . . .

Return to Index

AIxCC - Artificial Intelligence Cyber Challenge

Location: LVCC West/Floor 1/Hall 3/HW3-05-06 - Map
Home Page: https://aicyberchallenge.com/
Sched Page: https://aicyberchallenge.com/

PDT Times	Title	speaker
Friday		
11:30 - 11:50	SMOKE: Signature Management using Operational Know . . .	Tejas Patel
15:00 - 15:45	Closing the Software Vulnerability Gap	Dr. Kathleen Fisher
16:55 - 17:15	No Time for Complacency: The Stakes of AI in Cyber . . .	Heather Adkins
16:00 - 16:45	Industry Panel: The Modern Evolution of LLMs	Dr. Matt Turek,Heather Ad . . .
17:20 - 17:59	How Competitions Can Fuel Innovation	Mike Walker,Matt Knight,R . . .
Saturday		
10:00 - 10:45	Securing Health Care: AIxCC, DIGIHEALS, and UPGRAD . . .	Dr. Jennifer Roberts,Dr. . . .
11:30 - 11:50	Spotting Deepfakes in a World with Generative AI	Dr. William Corvey
14:30 - 14:59	Establishing the first Open Source Program Office . . .	Remy DeCausemaker
14:00 - 14:20	The Cat-and-Mouse Game of Adversarial Artificial I . . .	Alvaro Velasquez
15:45 - 16:30	A Reverse Engineer's Guide to AI Interpretability	Dr. Andrew Fasano
15:00 - 15:30	Contextualizing Open Source Software’s Importanc . . .	Aeva Black
17:15 - 17:59	Visualizing AIxCC: Bringing Your Code to Life	Mark Griffin
Sunday		
11:30 - 12:15	From research to release: Transferring AIxCC resul . . .	Dr. David A. Wheeler,Jeff . . .
13:15 - 13:59	The Challenge in Building a Challenge	

Return to Index

APV - AppSec Village

Location: LVCC West/Floor 2/W228-W230 - Map
Home Page: https://www.appsecvillage.com/
Sched Page: https://www.appsecvillage.com/events/dc-2024
DC Discord Chan: https://discord.com/channels/708208267699945503/790973922949726228

PDT Times	Title	speaker
Friday		
10:00 - 17:30	Fix the Flag Wargame	Harley Wilson
10:15 - 10:45	Winning big: AppSec Considerations From the Casino . . .	Aleise McGowan,Tennisha M . . .
11:00 - 12:59	Arsenal: AI Goat	Ofir Yakobi,Shir Sadon
11:00 - 12:59	Arsenal: CyberChef like Automation within BurpSuit . . .	Matthias Göhring,Florian . . .
11:00 - 13:59	Mind-Controlling Other Applications: An intro to i . . .	ILOVEPIE
11:00 - 11:30	Securing Frontends at Scale: Paving our Way to the . . .	Aaron Shim,jen-ozmen
11:45 - 12:15	Ticking SQLi	Iggy
11:00 - 12:59	Activity: Vulnerability Hunt - The Snippets Editio . . .	Mário Leitão-Teixeira
11:00 - 12:59	Activity: Spot the Secrets: Finding Secrets Throug . . .	mcdwayne
11:00 - 12:59	Activity: Spot the Reachable by Backslash	Czesia Glik,Yossi Pik
12:30 - 12:59	Hacking Corporate Banking for Fun and Profit	Charles Waterhouse,Nikhil . . .
13:00 - 13:59	Arsenal: GraphQL Armor - Open Source GraphQL Secur . . .	Antoine Carossio,Tristan . . .
13:15 - 13:45	SDLC Nightmares - Defeating Secure Code Review GPT . . .	Wang Zhilong,Xinzhi Luo
13:00 - 14:59	Activity: Capture the Container by Chainguard	Jonathan Leitschuh
13:00 - 14:59	Q&A With OWASP	
13:00 - 14:59	Activity: Test Your AppSec Knowledge by Deepfactor	Mike Larkin
14:45 - 15:15	Threat Modeling in the Age of AI	Adam Shostack
14:00 - 14:30	Relative Path File Injection: The Next Evolution i . . .	Ian Hickey
15:00 - 15:59	Arsenal: HunterBounter - Swiss Army Knife for Bug . . .	Utku Yildirim
15:00 - 15:59	Arsenal: Introducing RAVEN - Discovering and Analy . . .	Elad Pticha,Oreen Livni
15:00 - 17:30	The Open Source Fortress: Finding Vulnerabilities . . .	iosifache
15:30 - 15:59	Fine Grained Authorisation with Relationship-Based . . .	Ben Dechrai
15:00 - 16:59	Activity: Spot the Secrets: Finding Secrets Throug . . .	mcdwayne
15:00 - 16:59	Activity: Hacking Developers' Trust – Faking G . . .	Tal Folkman,Ori Ron,Mári . . .
16:15 - 16:45	I've got 99 problems but a prompt injection ain't . . .	Chloé Messdaghi,Kasimir . . .
17:00 - 17:30	When Chatbots Go Rogue – Lessons Learned from Bu . . .	Andra,Javan Rasokat
Saturday		
10:00 - 17:30	Fix the Flag Wargame	Harley Wilson
10:15 - 10:55	Navigating the Cyber Security Labyrinth: Choose Yo . . .	punkcoder
11:00 - 11:59	Arsenal: SCAGoat	Gaurav Joshi,HK,kvprashan . . .
11:00 - 13:59	Application Threat Modeling with Trike	AreTillery
11:40 - 12:10	Unlocking the Gates - Understanding Authentication . . .	Vikas Khanna
11:00 - 11:30	BOLABuster: Harnessing LLMs for Automating BOLA De . . .	Jay Chen,Ravid Mazon
11:00 - 12:59	Activity: Vulnerability Hunt - The Snippets Editio . . .	Mário Leitão-Teixeira

PDT Times	Title	speaker
11:00 - 12:59	Activity: API Security 101: Testing and Trivia by . . .	Ankush Jain,Ankita Gupta
11:00 - 12:59	Activity: Capture the Container by Chainguard	Jonathan Leitschuh
12:20 - 12:50	Maturing Your Application Security Program	SheHacksPurple
13:00 - 14:30	Arsenal: SanicDNS	Jasper Insinger
13:00 - 13:45	Transforming AppSec: Protecting 'Everything as Cod . . .	Kunal Bhattacharya,Sara A . . .
13:00 - 14:59	Activity: Spot the Reachable by Backslash	Czesia Glik,Yossi Pik
13:00 - 14:59	Activity: Spot the Secrets: Finding Secrets Throug . . .	mcdwayne
14:40 - 15:10	Engineers & Exploits: The Quest for Security	Andra,Spyros Gasteratos
14:00 - 14:30	Web2 Meets Web3: Hacking Decentralized Application . . .	Peiyu Wang
15:00 - 16:59	Injecting and Detecting Backdoors in Code Completi . . .	Ori Ron,Tal Folkman
15:20 - 15:50	Speed Bumps and Speed Hacks: Adventures in Car Man . . .	David Sopas,Paulo A. Silv . . .
15:00 - 16:59	Activity: Spot the Reachable by Backslash	Czesia Glik,Yossi Pik
15:00 - 16:59	Activity: API Security 101: Testing and Trivia by . . .	Ankush Jain,Ankita Gupta
16:40 - 17:10	0.0.0.0 Day: Exploiting Localhost APIs From The Br . . .	Avi Lumelsky,Gal Elbaz
16:00 - 16:30	The Missing Link - How we collect and leverage SBO . . .	Cassie Crossley
17:20 - 17:50	The Dark Side of Bug Bounty	Jason Haddix
Sunday		
10:45 - 12:59	Kubernetes Security: Hands-On Attack and Defense	alevsk
10:00 - 12:59	Fix the Flag Wargame	Harley Wilson
10:15 - 10:45	The Immortal Retrofuturism of Mainframe Computers . . .	Michelle Eggers
11:00 - 12:59	Arsenal: Kubescape - OSS security from left to rig . . .	ben@armosec.io
11:45 - 12:15	Your CI/CD Pipeline Is Vulnerable, But It's Not Yo . . .	Elad Pticha,Oreen Livni
11:00 - 11:30	Gridlock: The Dual-Edged Sword of EV and Solar AP . . .	Vangelis Stykas
11:00 - 12:59	Activity: Hacking Developers' Trust – Faking G . . .	Tal Folkman,Ori Ron,Mári . . .
11:00 - 12:59	Activity: Threat modelling fun session with OWASP . . .	Andra
11:00 - 12:59	Activity: Threat modelling fun session with OWASP . . .	Konstantinos Papapanagiot . . .
12:30 - 12:59	Using EPSS for Better Vulnerability Management	jgamblin

Return to Index

ASV - Aerospace Village

Location: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map
Home Page: https://aerospacevillage.org/
Sched Page: https://www.aerospacevillage.org/defcon-32-talk-schedule
DC Discord Chan: https://discord.com/channels/708208267699945503/732393044363444264

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Detect a Threat	TSA
10:00 - 17:59	Defend the Airport CTF	IntelliGenesis and IG Lab . . .
10:00 - 17:59	Darkstar Badge Challenge	Lockheed Martin
10:00 - 17:59	CubeSat Simulator	AMSAT
10:00 - 17:59	Bricks in the Air	
10:00 - 17:59	ARINC 664 CTF	Boeing
10:00 - 17:59	A-ISAC Aviation Cybersecurity Challenge	A-ISAC and Embry-Riddle A . . .
10:00 - 17:59	Hack-A-Sat Quals Challenges	Hack-A-Sat,Cromulence
10:00 - 17:59	Drone Capture the Flag (CTF)	Dark Wolf
10:00 - 17:59	Drone Flying Experience	Dark Wolf
10:00 - 17:59	Drone Hacking Activity	Dark Wolf
10:00 - 17:59	spacestudio and spacetower challenges	Exotrail,Hack-A-Sat
10:00 - 17:59	Space Systems Security CTF – Platform Security	CT Cubed
10:00 - 17:59	Drone Hacking Choose Your Own Adventure	Dark Wolf
10:00 - 17:59	Space Grand Challenge Luna	CalPoly
10:00 - 17:59	Selfie with a CubeSat	CalPoly
10:00 - 17:59	Hack-A-Sat Digital Twin	Hack-A-Sat,Cromulence
10:00 - 17:59	PTP Flight Challenge	Pen Test Partners
10:30 - 12:30	Building the Ultimate Budget-Friendly Low Earth Or . . .	Victor Fernandez Minguill . .
11:00 - 11:30	An adversarial approach to Airline Revenue Managem . . .	Craig Lester
11:30 - 11:59	Aviation cybersecurity lightning talk: Three topic . . .	Ken Munro
13:00 - 14:59	BYOS – Bring Your Own Satellite	Tim Fowler
15:30 - 17:30	Space Pirate Simulator	Michael Butler,Jacob Oakl . .
15:30 - 15:59	Ground Control to Major Threat - Hacking the Space . . .	Andrzej Olchawa
16:00 - 16:30	Analyzing the Security of Satellite-Based Air Traf . . .	Martin Strohmeier
Saturday		
10:00 - 17:59	spacestudio and spacetower challenges	Exotrail,Hack-A-Sat
10:00 - 17:59	Drone Hacking Activity	Dark Wolf
10:00 - 17:59	Hack-A-Sat Quals Challenges	Hack-A-Sat,Cromulence
10:00 - 17:59	Detect a Threat	TSA
10:00 - 17:59	PTP Flight Challenge	Pen Test Partners

PDT Times	Title	speaker
10:00 - 17:59	Selfie with a CubeSat	CalPoly
10:00 - 17:59	Hack-A-Sat Digital Twin	Hack-A-Sat,Cromulence
10:00 - 17:59	Space Grand Challenge Luna	CalPoly
10:00 - 17:59	Drone Capture the Flag (CTF)	Dark Wolf
10:00 - 17:59	Drone Hacking Choose Your Own Adventure	Dark Wolf
10:00 - 17:59	Space Systems Security CTF – Platform Security	CT Cubed
10:00 - 17:59	Drone Flying Experience	Dark Wolf
10:00 - 17:59	Defend the Airport CTF	IntelliGenesis and IG Lab . . .
10:00 - 17:59	Darkstar Badge Challenge	Lockheed Martin
10:00 - 17:59	CubeSat Simulator	AMSAT
10:00 - 17:59	Bricks in the Air	
10:00 - 17:59	ARINC 664 CTF	Boeing
10:00 - 17:59	A-ISAC Aviation Cybersecurity Challenge	A-ISAC and Embry-Riddle A . . .
10:30 - 11:30	Introduction to Drone Security	Hahna Kane Latonick
12:00 - 12:59	Secure the Skies: A Modern Android Security Resear . . .	Jonathan Waterman
12:30 - 12:59	GPS spoofing: it's about time, not just position	Ken Munro
13:30 - 14:30	Open Source Drone Hacking Simulator	Nick Aleks,Rudy Mendoza
13:00 - 13:30	Fly Catcher - How I Developed a Low-Cost Raspberry . . .	Angelina Tsuboi
13:30 - 13:59	Small Satellite Modeling and Defender Software	Kyle Murbach
14:15 - 14:59	RF Attacks on Aviation's Last Line of Defense Agai . . .	Giacomo Longo,Vincent Len . . .
16:00 - 16:59	Choose your own adventure: Has your fleet been hac . . .	Ken Munro
16:30 - 16:59	Offensive Security Testing: Safeguarding the Final . . .	Andrzej Olchawa
17:00 - 17:30	From Theory to Reality: Demonstrating the Simplici . . .	Randi Tinney
17:30 - 17:59	A dive into world of Aircraft PKI	Matt Gaffney
Sunday		
10:00 - 12:59	Hack-A-Sat Quals Challenges	Hack-A-Sat,Cromulence
10:00 - 12:59	Drone Hacking Activity	Dark Wolf
10:00 - 12:59	spacestudio and spacetower challenges	Exotrail,Hack-A-Sat
10:00 - 12:59	Drone Flying Experience	Dark Wolf
10:00 - 12:59	Space Systems Security CTF – Platform Security	CT Cubed
10:00 - 12:59	Drone Hacking Choose Your Own Adventure	Dark Wolf
10:00 - 12:59	Space Grand Challenge Luna	CalPoly
10:00 - 12:59	Selfie with a CubeSat	CalPoly
10:00 - 12:59	Hack-A-Sat Digital Twin	Hack-A-Sat,Cromulence
10:00 - 12:59	PTP Flight Challenge	Pen Test Partners
10:00 - 12:59	Drone Capture the Flag (CTF)	Dark Wolf
10:00 - 12:59	Detect a Threat	TSA
10:00 - 12:59	Defend the Airport CTF	IntelliGenesis and IG Lab . . .
10:00 - 12:59	Darkstar Badge Challenge	Lockheed Martin
10:00 - 12:59	CubeSat Simulator	AMSAT

PDT Times	Title	speaker
10:00 - 12:59	Bricks in the Air	
10:00 - 12:59	ARINC 664 CTF	Boeing
10:00 - 12:59	A-ISAC Aviation Cybersecurity Challenge	A-ISAC and Embry-Riddle A . . .
10:00 - 10:59	How to Corrupt Youth to Cyber Focused Space Scienc . . .	RC Jones
11:00 - 12:59	Watch The Skies: Build Your Own ADS-B receiver	Jim "Gurney" Ross
11:30 - 11:59	Warflying in a Cessna	Matt Thomassen,Sean McKee . . .
12:00 - 12:30	The Interplay between Safety and Security in Aviat . . .	Lillian Ash Baker
12:30 - 12:59	Behind the Badge: How we used and abused hardware . . .	Adam Batori,Robert Paffor . . .

Return to Index

BBV - Bug Bounty Village

Location: LVCC West/Floor 2/W215 - Map
Home Page: https://bugbountydefcon.com/
Sched Page: https://www.bugbountydefcon.com/agenda

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Caido Internals Deep-Dive	Emile Fugulin
10:00 - 10:59	Practical Exploitation of DoS in Bug Bounty	Roni "Lupin" Carta
11:00 - 12:15	Panel of Bug Bounty Community Leaders	Inti De Ceukelaire,Jessic . . .
11:00 - 11:59	From Easy Wins to Epic Challenges: Bounty Hunter E . . .	Daniel "Blaklis" Le Gall
12:15 - 13:45	A Zero to Hero Crash Course to Server-Side Request . . .	Ben "NahamSec" Sadeghipou . . .
14:00 - 14:59	Why You Should Be Hunting on Web3 Bug Bounties	Gonçalo Marques Raposo d . . .
15:00 - 16:30	Prototype Pollution in Depth, From Beginner to 0-D . . .	Lucas Philippe
16:30 - 17:59	LFG! Forming a Bug Bounty Hunting Party	Harrison Richardson
17:00 - 17:59	Reflections on a Decade in Bug Bounties: Experienc . . .	Charles Waterhouse,Nikhil . . .
Saturday		
10:00 - 10:59	Leveraging Internal Systems for Enhanced Bug Bount . . .	Rotem Bar
11:00 - 12:30	The Bug Hunters Methodology Live - DEF CON Edition	Jason Haddix
11:30 - 12:30	Hunters and Gatherers: A Deep Dive into the World . . .	Johnathan Kuskos,Katie Tr . . .
12:30 - 13:59	A Bug Hunter's Guide to Account Takeover	Ben "NahamSec" Sadeghipou . . .
14:30 - 15:59	High ROI Manual Bug Hunting Techniques	Justin "Rhynorater" Gardn . . .
14:00 - 14:30	Efficient Bug Bounty Automation Techniques	Gunnar Andrews
14:30 - 15:15	Leveraging AI for Smarter Bug Bounties	Diego Jurado,Joel "Nieman . . .
15:15 - 15:59	I've got 99 problems but a prompt injection ain't . . .	Chloé Messdaghi,Kasimir . . .
16:00 - 17:30	Unveiling Vulnerabilities: A Comprehensive Guide t . . .	Dhiyaneshwaran Balasubram . . .
17:00 - 17:59	Top War Stories from a TryHard Bug Bounty Hunter	Justin "Rhynorater" Gardn . . .
17:30 - 17:59	Meet the PortSwigger Research team (Q/A)	Martin Doyhenard,James "a . . .
Sunday		
11:00 - 12:30	Lost in Translation - WAF Bypasses By Abusing Data . . .	Ryan Barnett,Isabella Bar . . .

Return to Index

BHV - Bio Hacking Village

Location: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map
Home Page: https://www.villageb.io/
Sched Page: https://www.villageb.io/creatorstage2024
DC Discord Chan: https://discord.com/channels/708208267699945503/735273390528528415

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Biohacking Village: Device Lab	
15:30 - 15:59	Dysfunctional Unity: The Road to Nowhere	Michael "v3ga" Aguilar
15:00 - 15:30	Breaking Boundaries: Popping Shells in the Airgap . . .	Daniel Beard
Saturday		
10:00 - 10:59	Bridging Space and Medicine	Fernando De La Peña Llac . . .
10:00 - 17:59	Biohacking Village: Device Lab	
11:00 - 11:59	Eradicating Hepatitis C With BioTerrorism	Mixæl Swan Laufer
14:00 - 14:30	You got a lighter? I need to do some Electroporati . . .	James Utley,Joshua HIll,P . . .
14:30 - 15:15	The Past, Present, and Future of Bioweapons	Lucas Potter,Meow-Ludo Di . . .
15:30 - 16:30	D0N0H4RM: Cyber STEM Storytime	Nitin Natarajan,Christian . . .
Sunday		
10:00 - 12:59	Biohacking Village: Device Lab	
12:00 - 12:30	3DU: Homo (e)x Machina	Lacey Harbour

Return to Index

BICV - Blacks in Cybersecurity

Location: LVCC West/Floor 3/W314-W316 - Map
Home Page: https://www.blacksincyberconf.com/bic-village
Sched Page: https://www.blacksincyberconf.com/bic-village

PDT Times	Title	speaker
Friday		
09:30 - 09:59	BIC Village Opening Q&A with Marcus Hutchins	Michaela Barnett,Marcus H . . .
09:00 - 09:30	BIC United Kingdom Chapter Informational Virtual O . . .	Ike Marizu
10:00 - 10:59	BIC Village Keynote: Cyber Threat Landscape And La . . .	Kevin Parker
11:30 - 12:30	From Redlining to Weblining: Examining Broadband D . . .	Dr. Fatou Sankare
13:00 - 13:59	Worried about AI taking your job? Then this talk i . . .	Levone Campbell
14:00 - 14:59	"BYOCTF" - Bring Your Own [Challenges||Capture] Th . . .	Eli McRae
15:00 - 15:59	Life, Liberty and the pursuit of Convenience: the . . .	Kaleeque Pierce
16:00 - 16:59	The Implications of Cyberbiosecurity in Advanced A . . .	Simone Stephen
Saturday		
10:45 - 11:30	Unmasking Shadows: Strategies on Hunting Ransomwar . . .	R.J. McCarley
10:00 - 10:45	Fumbling into FedCyber	Nikkia Henderson
11:30 - 12:15	My Smart Red Team Copilot	Gaspard Baye
12:15 - 12:59	Weaponized Convenience: Inside the Rise of Remote . . .	Nader Zaveri,Fernando Tom . . .
13:00 - 13:59	Virtual SIEM/SOAR Workshop	Kenneth Ellington
13:00 - 13:59	Navigating Microaggressions and Fostering Inclusiv . . .	Jessica Hoffman
14:00 - 14:59	How to Find a 0day in iOS Apps	Xavier D. Johnson
14:00 - 14:59	MCPA x BIC x CAPT Virtual National Service Panel 2 . . .	Sydney Johns,Nikkia Hende . . .
15:00 - 15:59	FuzzLLM: A Fuzzing Framework for Discovering Jailb . . .	Ian G. Harris
16:00 - 16:59	The Transparency Algorithm: AI's Answer to Legal R . . .	Aquarious Workman
Sunday		
10:30 - 12:30	Ain’t that a Breach: Zero Trust Is the Only Solu . . .	Dr. Louis DeWeaver III
12:30 - 12:59	Exploring Bias in AI-Assisted News	Sydney Johns
13:00 - 13:59	Expanding Pathways into the National Cyber Workfor . . .	Ayan Islam

Return to Index

BTV - Blue Team Village

Home Page: https://blueteamvillage.org/
Sched Page: https://cfc.blueteamvillage.org/dc32/schedule/
DC Discord Chan: https://discord.com/channels/708208267699945503/732454317658734613

PDT Times	Title	speaker
Friday		
10:00 - 11:30	Building a Cyber Threat Intelligence Program from . . .	Apurv Singh Gautam,Karan . . .
10:00 - 10:30	Incident Response 101: Part 1 (IR Overview, Lifecy . . .	Jason Romero
10:30 - 10:59	Incident Response 101: Part 2 (Analyst Mindset and . . .	David "CountZ3r0" Roman
11:45 - 13:30	Adventures in Android Triage Collection	Omenscan
11:15 - 12:15	Cloud Native Security Platform for Defenders	Dafinga
12:30 - 13:30	Stealer Logs: Automation, Analysis, & Espionage in . . .	Eric Clay,Nick Ascoli
14:00 - 15:59	Area DC32: An Interactive Tabletop Takes Flight (A . . .	Aakin Patel,Caspian Kilke . . .
14:30 - 15:30	BTV Conversations: Exploring the Cyberpsychology o . . .	Todd Fletcher
15:30 - 16:30	BTV Conversations: Touch Grass to Combat Burnout	CtrlAltFu
17:00 - 17:59	CTI is Dead, Long Live CTI: Reassessing Blue Team' . . .	Aurora Johnson,Ben Goerz, . . .
Saturday		
10:00 - 11:59	Securing the Cloud with Cloud Threat Intelligence . . .	Natalie Simpson,Nivedita . . .
10:00 - 10:30	Obsidian: Forensics 101 Part 1	Sarthak Taneja
10:30 - 10:59	Obsidian: Forensics 101 Part 2	Sarthak Taneja
11:15 - 12:15	Use opensource AI to map alerts & logs into techni . . .	Ezz Tahoun
12:30 - 13:30	Introduction to Creating Osquery Extensions: Enhan . . .	Kivanc Aydin
12:30 - 13:30	From CTI to Creating Campaigns	Noah Lazzaro
14:00 - 14:59	Store bought is fine, sometimes!	Jason Craig,Lauren Proehl . . .
15:00 - 15:59	Hot SOC Topics for 2024: Feel the Spice!	Carson Zimmerman,Russ McR . . .
16:00 - 16:59	Thrunting or DEATH! (A BTV Panel)	Joe Slowik,Randy Pargman, . . .
17:00 - 17:59	Under the Hood: Incident Response at High Speed (A . . .	Angelo Violetti,David Zit . . .
Sunday		
10:30 - 11:59	Blue Team Careers: Do what you love, get paid for . . .	Cyb0rg42,Dani,Shea Nangle . . .
12:00 - 12:30	Blue Team Village Closing Ceremonies	

Return to Index

CHV - Car Hacking Village

Location: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map
Home Page: https://www.carhackingvillage.com/
Sched Page: https://www.carhackingvillage.com/defcon-32-talks
DC Discord Chan: https://discord.com/channels/708208267699945503/732722838942777474

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Car Hacking Village Activities	
13:30 - 13:59	Building a secure and resilient nationwide EV char . . .	Harry Krejsa,Sarah Hipel
13:00 - 13:30	V2GEvil: Ghost in the wires	Pavel Khunt,Thomas "Cr0wT . . .
14:00 - 14:30	UDSonCAN Attacks: Discovering Safety-Critical Risk . . .	Jonghyuk Song,Seunghee Ha . . .
14:30 - 14:59	How I discovered and hacked Learning Codes of the . . .	Danilo Erazo
15:00 - 15:30	Bluetooth Blues: Unmasking CVE 2023-52709 - The TI . . .	Kevin Mitchell
Saturday		
10:00 - 17:59	Car Hacking Village Activities	
16:00 - 16:30	Exploiting Bluetooth - from your car to the bank a . . .	Vladyslav Zubkov,Martin S . . .
16:30 - 16:59	Programming a CTS-V Gauge Cluster into an ATS-V, o . . .	Varjitt Jeeva
Sunday		
10:00 - 12:59	Car Hacking Village Activities	

Return to Index

CLV - Cloud Village

Location: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map
Home Page: https://cloud-village.org/
Sched Page: https://dc32.cloud-village.org/
DC Discord Chan: https://discord.com/channels/708208267699945503/732733373172285520

PDT Times	Title	speaker
Friday		
10:50 - 11:30	Catch them all! Detection Engineering and Purple T . . .	Christophe Tafani-Dereepe . . .
10:00 - 10:10	Opening Note	
10:10 - 10:50	Gone in 60 Seconds… How Azure AD/Entra ID Tenant . . .	Sean Metcalf
11:30 - 12:10	The Oracle Awakens: Demystifying Privilege Escalat . . .	Felipe Pr0teus,Lucas Ciof . . .
12:30 - 12:59	Cloud Offensive Breach and Risk Assessment (COBRA)	Harsha Koushik,Anand Tiwa . . .
12:10 - 12:30	One Port to Serve Them All - Google GCP Cloud Shel . . .	Hubert Lin
13:25 - 13:59	Exploit K8S via Misconfiguration .YAML in CSP envi . . .	Wooseok Kim,Changhyun Par . . .
13:00 - 13:25	ExploitIfNotExists: Privilege Escalation & Persist . . .	Zander Mackie
14:00 - 14:30	UnOAuthorized: Discovering the path to privilege e . . .	Eric Woodruff
14:30 - 15:10	Attacking and Defending Software Supply Chains: Ho . . .	Mike Ruth
15:10 - 15:40	Epyon - Attacking DevOps environments	Victor Pasknel
15:40 - 17:40	Hands-On Container Image Security: Mastering Sigst . . .	Mohammed Ilyas Ahmed,Syed . . .
Saturday		
10:30 - 11:10	Terraform Unleashed: Crafting Custom Provider Expl . . .	Alex Foley,Rupali
10:00 - 10:30	GCPwn: A Pentester's GCP Tool	Scott Weston
11:10 - 11:50	Identity Theft is not a Joke, Azure!	Karl Fosaaen
11:50 - 12:15	One Click, Six Services: Abusing The Dangerous Mul . . .	Liv Matan
12:15 - 12:40	Finding Holes in Conditional Access Policies	Brandon Colley
12:40 - 13:10	Revealing Choke Points: Practical Tactics for Boos . . .	Filipi Pires
13:50 - 15:50	Connecting the Dots: Mastering Alert Correlation f . . .	Ezz Tahoun
13:10 - 13:50	Runtime Reachability: Prioritizing Vulnerabilities . . .	Sam "Frenchie" Stewart
16:00 - 17:59	Exploiting common vulnerabilities in AWS environme . . .	Seth Art
Sunday		
10:00 - 10:35	Cloud Tripwires: fighting stealth with stealth	Jenko Hwong
10:35 - 11:10	Kicking in the Door to the Cloud: Exploiting Cloud . . .	Nick Frichette
11:10 - 11:45	Creating Azure Policy Compliant Backdoor	Viktor Gazdag
11:45 - 12:20	The Rise of the Planet of the Agents: LLM-based AI . . .	Roberto Rodriguez
12:20 - 12:40	Unexpected Leaks in AWS Transit Gateways	William Taylor
12:40 - 12:59	Closing Note	

Return to Index

CON - Contests

Home Page: https://defcon.outel.org/dcwp/dc32/activities/contests-list/
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_CON

PDT Times	Title	speaker
Thursday		
12:00 - 12:59	Hac-Man	
Friday		
09:00 - 16:59	Social Engineering Community Vishing Competition (. . .	
09:00 - 17:59	Social Engineering Community Youth Challenge	
10:00 - 17:59	IoT Village CTF	
10:00 - 17:59	Cloud Village CTF	
10:00 - 17:59	Hardware Hacking Village CTF	
10:00 - 17:59	Radio Frequency Capture the Flag	
10:00 - 17:59	Embedded CTF	
10:00 - 17:59	DARPA's Artificial Intelligence Cyber Challenge (A . . .	
10:00 - 17:59	Biohacking Village CTF	
10:00 - 17:59	QOLOSSUS	
10:00 - 17:59	ICS CTF	
10:00 - 14:59	Crash and Compile - Qualifications	
10:00 - 16:30	Car Hacking Village CTF	
10:00 - 17:59	HackFortress	
10:00 - 15:59	Beverage Chilling Contraption Contest	
10:00 - 16:59	Tinfoil Hat Contest	
10:00 - 17:59	Chasse Partie Systems CTF	
10:00 - 17:59	Gold Bug Challenge	
10:00 - 17:59	CrackMeIfYouCan	
10:00 - 17:59	DC’s Next Top Threat Model (DCNTTM)	
10:00 - 17:59	[CANCELED] AutoDriving CTF	
10:00 - 16:59	Red Team Village CTF	
10:00 - 17:59	Pinball High Score Contest	
10:00 - 17:59	5N4CK3Y Contest	
10:00 - 17:59	Hac-Man	
10:00 - 17:59	Darknet-NG	
10:00 - 17:59	? Cube	
10:30 - 17:59	Ham Radio Fox Hunt	Ham Radio Village Staff
10:00 - 17:59	Hacker Cooling Contraption Challenge, brought to y . . .	
10:00 - 17:59	PhreakMe presented by HackedExistence	
10:00 - 17:59	REALI7Y OVERRUN	
10:00 - 17:59	Lonely Hard Drive	
10:00 - 17:59	Lonely Tag	
10:00 - 17:59	spyVspy	

PDT Times	Title	speaker
10:00 - 17:59	DEF CON Scavenger Hunt	
10:00 - 17:59	Malware Contests: MARC I & BOMBE	
10:00 - 17:59	Live Recon Contest in Progress	
10:00 - 17:59	Adversary Wars CTF	
10:00 - 17:59	HTB CTF: Data Dystopia	
10:00 - 17:59	Octopus Game	
10:00 - 17:59	Cyber Defender - The Game	
10:00 - 17:59	CMD+CTRL at DEF CON 32	
10:00 - 17:59	Capture the Packet	
10:00 - 17:59	HardWired	
10:30 - 17:59	Blue Team Village CTF	
10:00 - 17:59	It's In That Place Where I Put That Thing That Tim . . .	
10:00 - 17:59	venator aurum - A Treasure Hunt	
10:00 - 23:59	Cloud Village CTF	
10:00 - 11:59	Gold Bug Challenge	
10:00 - 17:59	[CANCELED] AutoDriving CTF	
10:00 - 12:59	Radio Frequency Capture the Flag	
11:00 - 11:59	Betting on Your Digital Rights: 3rd Annual EFF Ben . . .	
11:00 - 11:59	CrackMeIfYouCan	
12:00 - 12:59	Gold Bug: Welcome	
12:00 - 19:59	DC Kubernetes Capture the Flag (CTF)	
12:00 - 16:59	Red Alert ICS CTF	
12:00 - 12:59	Aw, man…pages!	
12:00 - 17:59	Blacks in Cyber CTF	
12:00 - 17:59	Blacks in Cyber CTF	
12:00 - 16:59	Blacks in Cyber CTF	
12:00 - 16:59	Blacks in Cyber CTF	
13:00 - 17:59	Hacking Boundary Terminal	
13:00 - 14:59	AI Art Battle	
14:00 - 15:59	Hack3r Runw@y - Signups	
16:00 - 18:59	Pub Quiz	
18:30 - 19:30	Whose Slide Is It Anyway?	
20:00 - 21:59	Hacker Jeopardy	
Saturday		
10:00 - 17:59	IoT Village CTF	
10:00 - 17:59	Cloud Village CTF	
10:00 - 17:59	Hardware Hacking Village CTF	
10:00 - 17:59	Radio Frequency Capture the Flag	
10:00 - 17:59	Embedded CTF	
10:00 - 17:59	DARPA's Artificial Intelligence Cyber Challenge (A . . .	
10:00 - 17:59	Biohacking Village CTF	
10:00 - 17:59	QOLOSSUS	
10:00 - 17:59	ICS CTF	

PDT Times	Title	speaker
10:00 - 17:59	Car Hacking Village CTF	
10:00 - 17:59	HackFortress	
10:00 - 16:59	Tinfoil Hat Contest	
10:00 - 17:59	Chasse Partie Systems CTF	
10:00 - 17:59	CrackMeIfYouCan	
10:00 - 17:59	DC’s Next Top Threat Model (DCNTTM)	
10:00 - 17:59	[CANCELED] AutoDriving CTF	
10:00 - 16:59	Red Team Village CTF	
10:00 - 17:59	Pinball High Score Contest	
10:00 - 17:59	5N4CK3Y Contest	
10:00 - 17:59	Hac-Man	
10:00 - 17:59	Darknet-NG	
10:00 - 16:59	DC Kubernetes Capture the Flag (CTF)	
10:00 - 17:59	? Cube	
10:00 - 17:59	Ham Radio Fox Hunt	Ham Radio Village Staff
10:00 - 17:59	Hacker Cooling Contraption Challenge, brought to y . . .	
10:00 - 17:59	PhreakMe presented by HackedExistence	
10:00 - 17:59	REALI7Y OVERRUN	
10:00 - 17:59	Lonely Tag	
10:00 - 17:59	Lonely Hard Drive	
10:00 - 15:59	A Wall of Bribes	
10:00 - 17:59	spyVspy	
10:00 - 17:59	DEF CON Scavenger Hunt	
10:00 - 17:59	Malware Contests: MARC I & BOMBE	
10:00 - 12:59	Live Recon Contest in Progress	
10:00 - 17:59	Adversary Wars CTF	
10:00 - 17:59	HTB CTF: Data Dystopia	
10:00 - 17:59	Octopus Game	
10:00 - 17:59	Cyber Defender - The Game	
10:00 - 17:59	CMD+CTRL at DEF CON 32	
10:00 - 16:59	Red Alert ICS CTF	
10:00 - 17:59	HardWired	
10:00 - 17:59	Capture the Packet	
10:30 - 17:59	Blue Team Village CTF	
10:00 - 16:59	Blacks in Cyber CTF	
10:00 - 16:59	Blacks in Cyber CTF	
10:00 - 17:59	Social Engineering Community Youth Challenge	
10:00 - 17:59	venator aurum - A Treasure Hunt	
10:00 - 17:59	It's In That Place Where I Put That Thing That Tim . . .	
11:00 - 12:59	DEF CON 32 Beard and Mustache Contest	
12:00 - 17:59	Beverage Chilling Contraption Contest	
13:00 - 15:59	Live Recon Finalist Selection Process	
13:00 - 17:59	Hacking Boundary Terminal	

PDT Times	Title	speaker
13:00 - 14:59	Hack3r Runw@y	
14:00 - 14:59	Gold Bug: Puzzle Panel	
16:00 - 17:59	Live Recon Finalist Presentations	
16:00 - 18:59	Crash and Compile	
18:30 - 19:30	Feet Feud (Hacker Family Feud)	
20:00 - 21:59	Hacker Jeopardy	
Sunday		
10:00 - 12:59	IoT Village CTF	
10:00 - 12:59	Radio Frequency Capture the Flag	
10:00 - 12:59	Embedded CTF	
10:00 - 13:59	DARPA's Artificial Intelligence Cyber Challenge (A . . .	
10:00 - 12:59	Biohacking Village CTF	
10:00 - 12:59	QOLOSSUS	
10:00 - 12:59	ICS CTF	
10:00 - 11:59	Car Hacking Village CTF	
10:00 - 12:59	Chasse Partie Systems CTF	
10:00 - 17:59	Gold Bug Challenge	
10:00 - 11:59	Gold Bug Challenge	
10:00 - 10:59	CrackMeIfYouCan	
10:00 - 11:59	Red Team Village CTF	
10:00 - 12:59	Pinball High Score Contest	
10:00 - 11:59	5N4CK3Y Contest	
10:00 - 12:59	Hac-Man	
10:00 - 11:59	Darknet-NG	
10:00 - 11:59	? Cube	
10:00 - 12:59	Ham Radio Fox Hunt	Ham Radio Village Staff
10:00 - 12:59	Hacker Cooling Contraption Challenge, brought to y . . .	
10:00 - 12:59	PhreakMe presented by HackedExistence	
10:00 - 12:59	REALI7Y OVERRUN	
10:00 - 12:59	Lonely Hard Drive	
10:00 - 12:59	Lonely Tag	
10:00 - 11:59	A Wall of Bribes	
10:00 - 11:59	DEF CON Scavenger Hunt	
10:00 - 12:59	Malware Contests: MARC I & BOMBE	
10:00 - 11:59	Adversary Wars CTF	
10:00 - 12:59	HTB CTF: Data Dystopia	
10:00 - 12:59	Octopus Game	
10:00 - 11:59	Cyber Defender - The Game	
10:00 - 11:59	CMD+CTRL at DEF CON 32	
10:00 - 11:59	Capture the Packet	
10:00 - 12:59	HardWired	
10:00 - 12:59	venator aurum - A Treasure Hunt	

Return to Index

CPV - Crypto Privacy Village

Location: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map
Home Page: https://cryptovillage.org/
Sched Page: https://cryptovillage.org/
DC Discord Chan: https://discord.com/channels/708208267699945503/732734002011832320

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Differential privacy beyond algorithms: Challenges . . .	Rachel Cummings
10:00 - 10:02	CPV: Day 1 Welcome	
11:00 - 11:30	Travel Better: Expedient Digital Defense	Grey Fox
13:00 - 13:15	CPV: Intro to Cyphers	
13:30 - 13:45	Surprise Talk	Rachel Cummings
14:00 - 14:30	Data Brokers and the Threat to Your Privacy	Yael Grauer
15:00 - 15:30	Basic Mobile Phone Privacy	Grey Fox
16:00 - 16:59	Data On Demand: The challenges of building a priva . . .	Matt Domko
17:30 - 17:59	Fool us Once, fool us twice... Hacking Norwegian B . . .	Cecilie Wian,Per Thorshei . . .
Saturday		
10:25 - 10:30	CPV: Day 2 Welcome	
10:30 - 10:45	CPV: Intro to Cyphers	
12:30 - 12:59	Basic Mobile Phone Privacy	Grey Fox
13:00 - 13:15	CPV: Intro to Cyphers	
16:00 - 16:30	A Whirlwind Tour of the FBI's Secret Encrypted Cha . . .	Joseph Cox
17:30 - 17:59	GUR RIBYHGVBA BS PELCGBTENCUL	Jeff Man
17:00 - 17:30	Attacks on GenAI data and using vector encryption . . .	Bob Wall,Patrick Walsh
Sunday		
10:30 - 11:30	Famous and Not-So-Famous Unsolved Codes	Elonka Dunin,Klaus Schmeh
10:00 - 10:30	Porn & Privacy	ET
13:00 - 13:30	Wu-Tang is for the Children: How States Laws Inten . . .	Anthony Hendricks

Return to Index

DC - DEF CON Talks

Home Page: https://defcon.org/html/defcon-32/dc-32-speakers.html
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_DC

PDT Times	Title	speaker
Friday		
10:30 - 11:15	Spies and Bytes: Victory in the Digital Age	General Paul M. Nakasone
10:00 - 10:20	Welcome to DEF CON	Jeff "The Dark Tangent" M . . .
10:00 - 10:45	Mobile Mesh RF Network Exploitation: Getting the T . . .	Erwin Karincic,Woody
10:00 - 10:45	Where’s the Money: Defeating ATM Disk Encryption	Matt Burch
10:30 - 11:15	Defeating magic by magic Using ALPC security fea . . .	WangJunJie Zhang,YiSheng . . .
10:00 - 10:20	Securing CCTV Cameras Against Blind Spots	Jacob Shams
10:00 - 10:45	Behind Enemy Lines: Going undercover to breach the . . .	Jon DiMaggio
11:30 - 11:59	Atomic Honeypot: A MySQL Honeypot That Drops Shell . . .	Alexander Rubin,Martin Ra . . .
11:30 - 12:15	Listen to the whispers: web timing attacks that ac . . .	James "albinowax" Kettle
11:00 - 11:20	No Symbols When Reversing? No Problem: Bring Your . . .	Max "Libra" Kersten
11:30 - 12:45	High Intensity Deconstruction: Chronicles of a Cry . . .	Babak Javadi,Aaron Levy,N . . .
11:30 - 12:30	Custom, cheap, easy, and safe badges - without sta . . .	Joe "securelyfitz" FitzPa . . .
11:00 - 11:45	The XZ Backdoor Story: The Undercover Operation Th . . .	Thomas Roccia
12:00 - 12:45	Fireside Chat with DNSA Anne Neuberger	Anne Neuberger,Jeff "The . . .
12:00 - 12:45	On Your Ocean's 11 Team, I'm the AI Guy (technical . . .	Harriet Farlow
12:30 - 13:15	Kicking in the Door to the Cloud: Exploiting Cloud . . .	Nick Frichette
12:00 - 13:15	Veilid Dev and Community Meetup	The_Gibson
13:00 - 13:45	If Existing Cyber Vulnerabilities Magically Disapp . . .	Dr. Stefanie Tompkins,Dr. . . .
13:00 - 13:45	Sshamble: Unexpected Exposures in the Secure Shell	HD Moore,Rob King
13:30 - 14:15	Digital Emblems: When markings are required under . . .	Bill Woodcock
13:00 - 13:45	Defeating EDR Evading Malware with Memory Forensic . . .	Andrew Case,Austin Seller . . .
13:30 - 14:15	Xiaomi The Money - Our Toronto Pwn2Own Exploit and . . .	Ken Gannon,Ilyes Beghdadi
14:00 - 14:45	DEF CON Unplugged: Cocktails & Cyber with Jeff & J . . .	Jen Easterly
14:00 - 14:45	Optical Espionage: Using Lasers to Hear Keystrokes . . .	samy kamkar
14:30 - 15:15	Breaching AWS Accounts Through Shadow Resources	Yakir Kadkoda,Michael Kat . . .
14:00 - 14:45	The Way To Android Root: Exploiting Your GPU On Sm . . .	Xiling Gong,Eugene Rodion . . .
14:30 - 15:15	Joe and Bruno's Guide to Hacking Time: Regeneratin . . .	Joe "Kingpin" Grand,Bruno . . .
15:00 - 15:59	DC101 Panel	Nikita Kronenberg,Drew "a . . .
15:00 - 15:45	Abusing Windows Hello Without a Severed Hand	Ceri Coburn,Dirk-jan Moll . . .
15:30 - 16:15	Taming the Beast: Inside the Llama 3 Red Team Proc . . .	Aaron "dyn" Grattafiori,I . . .
15:00 - 15:45	Android App Usage and Cell Tower Location: Private . . .	Ryan Johnson
15:30 - 16:15	Social Engineering Like you’re Picard	Jayson E. Street
16:00 - 16:59	Making the DEF CON 32 Badge	Mar Williams
16:00 - 16:45	Eradicating Hepatitis C With BioTerrorism	Mixæl Swan Laufer
16:30 - 17:15	Leveraging private APNs for mobile network traffic . . .	Aapo Oksman
16:00 - 16:45	Outlook Unleashing RCE Chaos: CVE-2024-30103 & CVE . . .	Michael Gorelik ,Arnold O . . .

PDT Times	Title	speaker
16:30 - 17:15	Why are you still, using my server for your intern . . .	Thomas Boejstrup Johansen
17:00 - 17:45	Bricked & Abandoned: How To Keep The IoT From Beco . . .	Paul Roberts,Chris Wysopa . . .
17:00 - 17:45	One for all and all for WHAD: wireless shenanigans . . .	Damien Cauquil,Romain Cay . . .
17:30 - 18:15	Exploiting Bluetooth - from your car to the bank a . . .	Vladyslav Zubkov,Martin S . . .
17:00 - 17:45	Breaking Secure Web Gateways (SWG) for Fun and Pro . . .	Vivek Ramachandran,Jeswin . . .
17:30 - 17:50	Stranger in a Changed Land	Tony Sager
18:00 - 18:20	DEF CON Franklin Project	Jacob H Braun
Saturday		
10:00 - 10:45	The Pwnie Awards	
10:30 - 11:15	Gotta Cache ‘em all: bending the rules of web ca . . .	Martin Doyhenard
10:00 - 10:20	Laundering Money	Michael Orlitzky
10:00 - 10:20	Mutual authentication is optional	Xavier Zhang
10:30 - 11:15	Smishing Smackdown: Unraveling the Threads of USPS . . .	S1nn3r
10:00 - 10:45	Reverse Engineering MicroPython Frozen Modules: Da . . .	Wesley McGrew
10:00 - 11:45	CULT OF THE DEAD COW & Friends Present: Prime Cuts . . .	Deth Veggie,Walter J. Sch . . .
11:00 - 11:45	The Rise and Fall of Binary Exploitation	Stephen Sims
11:30 - 12:15	QuickShell: Sharing is caring about an RCE attack . . .	Or Yair,Shmuel Cohen
11:30 - 12:15	Sudos and Sudon’ts - Peering inside Sudo for Win . . .	Michael "mtu" Torres
11:00 - 11:45	SHIM me what you got - Manipulating Shim and Offic . . .	Ron Ben-Yizhak,David Shan . . .
12:00 - 12:45	Disenshittify or die! How hackers can seize the me . . .	Cory Doctorow
12:30 - 13:15	The Secret Life of a Rogue Device - Lost IT Assets . . .	Matthew "mandatory" Bryan . . .
12:30 - 13:15	AMD Sinkclose: Universal Ring -2 Privilege Escalat . . .	Enrique Nissim,Krzysztof . . .
12:00 - 12:45	Grand Theft Actions: Abusing Self-Hosted GitHub Ru . . .	Adnan Khan,John Stawinski
12:00 - 12:59	The wild and wonderful world of early Microprocess . . .	Michael Brown
12:00 - 12:45	automobiles, alcohol, blood, sweat, and creative r . . .	atlas
13:00 - 13:45	Fireside Chat with Jay Healey and National Cyber D . . .	Harry Coker Jr.,Jay Heale . . .
13:30 - 14:15	NTLM - The Last Ride	Jim Rush,Tomais Williamso . . .
13:30 - 14:15	Behind Enemy Lines: Engaging and Disrupting Ransom . . .	Vangelis Stykas
13:00 - 13:45	OH-MY-DC: Abusing OIDC all the way to your cloud	Aviad Hahami
13:00 - 13:59	All Your Keyboards Are Belong to US!	Federico Lucifredi
13:00 - 14:59	Learn Zero Trust Network Security with Cloudflare	
13:00 - 13:45	Inside the FBI’s Secret Encrypted Phone Company . . .	Joseph Cox
14:00 - 14:45	SQL Injection Isn't Dead: Smuggling Queries at the . . .	Paul Gerste
14:30 - 15:15	Troll Trapping Through TAS Tools - Exposing Speedr . . .	Allan "dwangoAC" Cecil
14:30 - 15:15	ACE up the Sleeve: From getting JTAG on the iPhone . . .	Thomas "stacksmashing" Ro . . .
14:00 - 14:45	Discovering and exploiting local attacks against t . . .	Jeffrey Hofmann,Colby Mor . . .
14:00 - 14:45	Hacking Millions of Modems (and Investigating Who . . .	Sam Curry
15:00 - 15:45	Exploiting the Unexploitable: Insights from the Ki . . .	Mikhail Shcherbakov
15:30 - 16:15	HookChain: A new perspective for Bypassing EDR Sol . . .	Helvio Carvalho Junior
15:30 - 16:15	Unsaflok: Hacking millions of hotel locks	Lennert Wouters,Ian Carro . . .
15:00 - 15:45	Measuring the Tor Network	Silvia Puglisi,Roger Ding . . .
15:00 - 15:59	Real life hacking stories (that can’t be recorde . . .	
15:00 - 15:45	A Shadow Librarian in Broad Daylight: Fighting bac . . .	Daniel Messer

PDT Times	Title	speaker
16:30 - 17:15	Watchers being watched: Exploiting the Surveillanc . . .	Chanin Kim,Myeonghun Pak, . . .
16:00 - 16:20	Compromising an Electronic Logging Device and Crea . . .	Jake Jepson,Rik Chatterje . . .
16:30 - 17:15	DEF CON Academy: Cultivating M4D SK1LLZ In the DEF . . .	Yan "Zardus" Shoshitaishv . . .
16:30 - 17:15	Breaking the Beam: Exploiting VSAT Satellite Modem . . .	Vincent Lenders,Johannes . . .
16:00 - 16:45	Secrets and Shadows: Leveraging Big Data for Vulne . . .	Bill Demirkapi
16:00 - 16:45	Encrypted newspaper ads in the 19th century - The . . .	Elonka Dunin,Klaus Schmeh
17:30 - 18:15	Iconv, set the charset to RCE: exploiting the glib . . .	Charles "cfreal" Fol
17:00 - 17:20	Techniques for Creating Process Injection Attacks . . .	Bramwell Brizendine,Shiva . . .
17:30 - 18:15	Nano-Enigma: Uncovering the Secrets Within eFuse M . . .	Michal Grygarek,Martin Pe . . .
17:00 - 17:59	Quantum Leap: The future of Computing and the secu . . .	
17:00 - 17:45	A Treasure Trove of Failures: What History's Gre . . .	Pete Stegemeyer
Sunday		
10:00 - 10:45	Splitting the email atom: exploiting parsers to by . . .	Gareth Heyes
10:00 - 10:45	AWS CloudQuarry: Digging for secrets in public AMI . . .	Eduard Agavriloae,Matei J . . .
10:00 - 10:45	Windows Downdate: Downgrade Attacks Using Windows . . .	Alon Leviev
10:00 - 10:20	Unlocking the Gates: Hacking a secure Industrial R . . .	Moritz Abrell
10:30 - 11:15	Changing Global Threat Landscape with Rob Joyce an . . .	Rob Joyce,Jeff "The Dark . . .
10:00 - 10:59	Taking off the blindfold: Detecting persistent thr . . .	Gastón Aznarez,Octavio G . . .
10:00 - 10:45	The not-so-silent type: Breaking network crypto in . . .	Jeffrey Knockel,Mona Wang
11:00 - 11:45	(|(MaLDAPtive:¯_(LDAP)_/¯=ObFUsc8t10n) (De-Obfu . . .	Daniel Bohannon,Sabajete . . .
11:00 - 11:45	The hack, the crash and two smoking barrels. (And . . .	Thomas "Cr0wTom" Sermpini . . .
11:00 - 11:45	Dragon SlayingGuide: Bug Hunting In VMware Device . . .	JiaQing Huang,Hao Zheng,Y . . .
11:30 - 12:15	Open sesame - or how vulnerable is your stuff in e . . .	Dennis Giese,Braelynn
11:00 - 11:45	Deception & Counter Deception – Defending Yourse . . .	Tom "Decius" Cross,Greg C . . .
12:00 - 12:45	DriverJack: Turning NTFS and Emulated Read-only Fi . . .	Alessandro Magnosi
12:30 - 13:15	Redefining V2G - How to use your vehicle as a game . . .	Timm Lauser,Jannis Hambor . . .
12:30 - 13:15	AIxCC Closing Ceremonies	Andrew Carney,Perri Adams
12:00 - 12:20	Solving the "Lover, Stalker, Killer" Murder with s . . .	Anthony Kava
12:30 - 13:15	Clash, Burn, and Exploit: Manipulate Filters to Pw . . .	Kuan-Ting "HexRabbit" Che . . .
13:00 - 13:45	Your AI Assistant has a Big Mouth: A New Side-Chan . . .	Yisroel Mirsky,Roy Weiss, . . .
13:30 - 14:15	Incubated Machine Learning Exploits: Backdooring M . . .	Suha Sabi Hussain
13:30 - 14:45	Contest Closing Ceremonies and Awards	
13:30 - 14:15	Bringing Down North Korea	Alejandro Caceres
14:00 - 14:45	Abusing legacy railroad signaling systems	David Meléndez,Gabriela . . .
15:00 - 17:45	DEF CON Closing Ceremonies & Awards	Jeff "The Dark Tangent" M . . .

Return to Index

DCG - DEF CON Groups

PDT Times	Title	speaker
Friday		
10:00 - 17:59	DEF CON Groups - Open for questions and hanging ou . . .	
Saturday		
10:00 - 17:59	DEF CON Groups - Open for questions and hanging ou . . .	
Sunday		
10:00 - 12:59	DEF CON Groups - Open for questions and hanging ou . . .	

Return to Index

DCGVR - DEF CON Groups VR

Home Page: https://www.dcgvr.org/
Sched Page: https://www.dcgvr.org/

PDT Times	Title	speaker
Saturday		
10:00 - 10:30	Jayson Street - Keynote	Jayson E. Street
10:00 - 10:30	Jayson Street - Keynote	Jayson E. Street
11:00 - 11:40	Breaking and Defending Cloud Infrastructure: Red T . . .	Amal Joy,Abhishek S
12:05 - 13:05	DEF CON Groups Panel #1	ET E,xray,TX,over . . .
13:05 - 14:05	The Sand Castle - The State of the MacOS Sandbox	Jonathan "JBO" Bar Or
14:05 - 14:50	Brief History of GRC	Allen Baranov
15:05 - 16:05	How I Learned to Stop Worrying and Love the Ban	Manfred
16:05 - 17:05	Unlocking Hidden Superpowers: Neurodiversity in In . . .	Xavier "rubix1138" Ashe
17:05 - 17:50	Front line first aid: Triaging your DFIR emergency . . .	Neumann "scsideath" Lim
18:05 - 19:05	Something something Meshtastic Pip-Boy Personal Me . . .	Giglio
19:05 - 19:30	Who cashed my check?! Catching (Very Obvious) Frau . . .	Squiddy
19:35 - 19:50	Shifting left in Reversing apk by converting smali . . .	Just Tulpa
20:05 - 20:35	What!? Is my life that fragile?	hoodiePony

Return to Index

DDV - Data Duplication Village

Location: LVCC West/Floor 2/W225 - Map
Home Page: https://dcddv.org/
Sched Page: https://dcddv.org/dc32-schedule
DC Discord Chan: https://discord.com/channels/708208267699945503/732732641694056478

PDT Times	Title	speaker
Thursday		
16:00 - 19:59	DDV starts accepting drives for duplication	
Friday		
10:00 - 16:59	DDV open and accepting drives for duplication	
Saturday		
10:00 - 16:59	DDV open and accepting drives for duplication	
Sunday		
10:00 - 10:59	Last chance to pick up drives at the DDV	

Return to Index

DL - DEF CON DemoLabs

Home Page: https://forum.defcon.org/node/248122
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_DL

PDT Times	Title	speaker
Friday		
10:00 - 11:45	Docker Exploitation Framework	Emmanuel Law,Rohit Pitke
10:00 - 11:45	Zip It Up, Sneak It In - Introduction of apkInspec . . .	Kaloyan Velikov,Leonidas . . .
10:00 - 11:45	Volatile Vault - Data Exfiltration in 2024	Moritz Laurin Thomas,Patr . . .
10:00 - 11:45	Bluetooth Landscape Exploration & Enumeration Plat . . .	Paul Wortman
10:00 - 11:45	Nebula - 3 Years of Kicking *aaS and Taking Userna . . .	Bleon Proko
10:00 - 11:45	Cloud Offensive Breach and Risk Assessment (COBRA)	Anand Tiwari,Harsha Koush . . .
12:00 - 13:45	distribRuted - Distributed Attack Framework	Ismail Melih Tas,Numan Oz . . .
12:00 - 13:45	BypassIT - Using AutoIT & Similar Tools for Covert . . .	Ezra Woods,Mike Manrod
12:00 - 13:45	Tengu Marauder	Leonardo Serrano,Lexie Th . . .
12:00 - 13:45	Skynet	Craig Chamberlain,Rewanth . . .
12:00 - 13:45	The World Wide Paraweb	Nathan Sidles
12:00 - 13:45	Serberus	Patrick Kiley
14:00 - 15:45	Automated Control Validation with Tommyknocker	Jeremy Banker
14:00 - 15:45	HIDe & SEEK	Jonathan Fischer,Matthew . . .
14:00 - 15:45	SCAGoat - Exploiting Damn Vulnerable SCA Applicati . . .	Hare Krishna Rai,Prashant . . .
14:00 - 15:45	Garak	Erick Galinkin,Leon Dercz . . .
14:00 - 15:45	XenoboxX - Hardware Sandbox Toolkit	Cesare Pizzi
14:00 - 15:45	Hopper - Distributed Fuzzer	Luciano Remes,Wade Cappa
Saturday		
10:00 - 11:45	Maestro	Chris Thompson
10:00 - 11:45	Tempest	Kirk Trychel
10:00 - 11:45	5Ghoul Framework - 5G NR Attacks & 5G OTA Fuzzing	Matheus Eduardo Garbelini . . .
10:00 - 11:45	Testbed Virtual Factory	Borja Pintos Castro,Camil . . .
10:00 - 11:45	Cyber Security Transformation Chef (CSTC)	Florian Haag,Matthias Gö . . .

PDT Times	Title	speaker
10:00 - 11:45	MITRE Caldera	Mark Perry,Rachel Murphy
12:00 - 13:45	Open Hardware Design for BusKill Cord	Melanie Allen
12:00 - 13:45	The Metasploit Framework v6.4	Jack Heysel,Spencer McInt . . .
12:00 - 13:45	CODASM - Hiding Payloads in Plain .text	Moritz Laurin Thomas
12:00 - 13:45	GC2 - The First Serverless Command & Control	Lorenzo Grazian
12:00 - 13:45	MPT - Pentest in Action	Jyoti Raval
12:00 - 13:45	FACTION	Josh Summitt
14:00 - 15:45	MITRE Caldera for OT	Blaine Jeffries,Devon Col . . .
14:00 - 15:45	Vovk - Advanced YARA Rule Generator v2.0	Benjamyn Whiteman,Vishal . . .
14:00 - 15:45	TheAllCommander 2.0	Matthew Handy
14:00 - 15:45	Drop-Pi	Doug Kent,Robert Ditmer
14:00 - 15:45	Moriarty	Anthony “Coin” Rose,J . . .
14:00 - 15:45	Farming Ndays with GreyNoise	Andrew Morris

Return to Index

ESV - Embedded Systems Village

Location: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map
Home Page: https://embeddedvillage.org/

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Secure Microcontroller Workshop	
10:00 - 17:59	Emulating (and Hacking) Embedded Devices	
10:00 - 17:59	Wireless & Networking workshop	Alex Kelly
10:00 - 17:59	101 Labs: Firmware and Software exploitation	
10:00 - 17:59	101 Labs: Hardware Lab	
10:00 - 17:59	Hardware Hacking: Glitching Lab	
Saturday		
10:00 - 17:59	101 Labs: Hardware Lab	
10:00 - 17:59	Hardware Hacking: Glitching Lab	
10:00 - 17:59	101 Labs: Firmware and Software exploitation	
10:00 - 17:59	Secure Microcontroller Workshop	
10:00 - 17:59	Emulating (and Hacking) Embedded Devices	
10:00 - 17:59	Wireless & Networking workshop	Alex Kelly
15:15 - 15:59	Reverse engineering and hacking Ecovacs robots	Dennis Giese,Braelynn
Sunday		
10:00 - 12:59	Secure Microcontroller Workshop	
10:00 - 12:59	Emulating (and Hacking) Embedded Devices	
10:00 - 12:59	Wireless & Networking workshop	Alex Kelly
10:00 - 12:59	101 Labs: Hardware Lab	
10:00 - 12:59	Hardware Hacking: Glitching Lab	
10:00 - 12:59	101 Labs: Firmware and Software exploitation	

Return to Index

HDA - DEF CON Hackers with Disabilities

PDT Times	Title	speaker
Thursday		
10:00 - 17:59	HDA Community - Open for Accessibility Questions/H . . .	
Friday		
10:00 - 23:59	HDA Community - Open for Accessibility Questions/H . . .	
14:00 - 15:59	HDA Presents : Naomi Brockwell	Naomi Brockwell
18:00 - 23:59	HDA Chillout w/ Dj Delchi	
Saturday		
10:00 - 23:59	HDA Community - Open for Accessibility Questions/H . . .	
12:00 - 15:59	HDA Presents the open Synth Jam Session	
Sunday		
10:00 - 14:59	HDA Community - Open for Accessibility Questions/H . . .	

Return to Index

HRV - Ham Radio Village

Location: LVCC West/Floor 3/W321 - Map
Home Page: https://hamvillage.org/
Sched Page: https://hamvillage.org/dc32/index.html
DC Discord Chan: https://discord.com/channels/708208267699945503/732733631667372103

PDT Times	Title	speaker
Thursday		
10:00 - 16:59	Ham in a Day Class	Dan "dan_kb6nu" Romanchik
Friday		
11:30 - 12:30	SSTV: How To Send Cat Memes Via Ham Radio	Hamster
13:00 - 15:59	Ham Radio Exams	
14:00 - 14:59	Hacking the Quansheng UV-K5	Jon Marler
Saturday		
11:00 - 16:59	Ham Radio Exams	
11:00 - 11:59	Ham Radio for Hackers	Dan "dan_kb6nu" Romanchik
13:00 - 13:30	Staying alive off the grid - using APRS and Lambda . . .	Kamikazi
14:00 - 14:30	Low Power & Long Range Communications - QRP	Escobar
15:00 - 15:30	Clapping cheeks, aka home brew antennas	Seth
16:00 - 16:30	Ham Radio in an HOA: Radio in the Face of Your Opp . . .	Danny Quist
Sunday		
10:00 - 13:30	Ham Radio Exams	
11:00 - 11:30	Basic Packet Radio Operation	Jeremy
11:30 - 11:59	Advanced Packet Radio Operation	Jeremy

Return to Index

ICSV - Industrial Control Systems Village

Location: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map
Home Page: https://www.icsvillage.com/
Sched Page: https://www.icsvillage.com/defconevents/def-con-32
DC Discord Chan: https://discord.com/channels/708208267699945503/735938018514567178

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Does the World Need Another Threat Model, the Road . . .	Niyo Little Thunder Pears . . .
10:30 - 10:59	Attack and Defence in OT - Simulating attacks agai . . .	Julia Dewitz-Würzelberge . . .
10:00 - 10:50	Using ChatGPT to Write Defensive & Offensive Tools . . .	Mike Holcomb
11:00 - 11:25	Importance of ICS knowledge from a engineer's pers . . .	Ray Baeza
11:30 - 11:55	Invisible Invaders: Strategies to Combat Living Of . . .	Dan Gunter
12:00 - 12:59	A hole in one: pwning a cruise ship from a golf si . . .	Andrew Tierney
13:00 - 13:25	HandPwning: "Your Hand is your Passport. Verify me . . .	Luca "CYBERANTANI" Bongio . . .
13:30 - 13:55	Cyber Informed Engineering for Critical Infrastruc . . .	Aaron Crow
14:00 - 14:30	The Risk and Reward of Distributed Industrial Cont . . .	Joe Slowik
14:30 - 14:59	Mapping the Landscape: Top 10 Cybersecurity Trends . . .	Mars Cheng
14:00 - 14:55	Detouring Danger: Hunting Privileged File Operatio . . .	Asher Davila
15:00 - 15:25	The People's Republic of Fieldbus: What to know ab . . .	Jonathan Reiter
15:30 - 15:55	OT Incident response and Threat Hunting	Adam Robbie,Bradley Nash
16:00 - 16:55	Correlating & contextualizing OT events/alerts/log . . .	Ezz Tahoun
16:30 - 16:59	ICS 101	Bryson Bort ,Tom VanNorma . . .
Saturday		
10:00 - 10:55	Securing the Harvest: Cyber Defense for Agricultur . . .	Ray Baeza
11:00 - 11:50	Where's Waldo? Can you find the Raspberry Pi in th . . .	Shane McFly,Brian Howard
12:00 - 12:30	I am still the Captain now!	Paul Brownridge
12:30 - 12:59	Manufacturing- Lessons Learned, Lessons Taught	Tim Chase
12:00 - 12:59	Don't Give Up The Ship! Maritime SOC/NOC Afloat	Philip Acosta,Cliff Neve, . . .
13:30 - 13:55	The perma-lag: why industrial cybersecurity will n . . .	Kyle McMillan
13:00 - 13:25	Don't Ship Your Bridges! Tools to Explore Wireless . . .	Nick Halt,Duncan Woodbury
14:00 - 14:50	Seeing the Unseen: An Evaluation of Active Scannin . . .	Jennifer Guerra
15:00 - 15:30	War Games: Red Team for OT (Based on Real World Ca . . .	Shishir Gupta
15:30 - 15:55	Building Zero Trust in ICS	Sting
15:00 - 15:30	Underway to Identifying Commonalities of Cybersecu . . .	Rebecca J. Rohan
16:00 - 16:50	Product security considerations for OT security ap . . .	Brandon Dudley,Robert Lan . . .
Sunday		
10:00 - 10:55	Countdown to Industrial Extinction	Mike Holcomb
11:00 - 11:50	Tracking Industrial Advanced Threat Actors Who Are . . .	Ron Fabela
12:00 - 12:59	Building a foundation with the 5 critical controls	Dillon Lee
13:30 - 13:55	Forgetting the Fundamentals? Data Communications: . . .	Kevin Manna
13:00 - 13:25	Career Development - The Human Element	Kirsten Renner

Return to Index

IOTV - Internet Of Things Village

Location: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map
Home Page: https://www.iotvillage.org/
Sched Page: https://www.iotvillage.org/defcon.html#Talks
DC Discord Chan: https://discord.com/channels/708208267699945503/732734565604655114

PDT Times	Title	speaker
Friday		
10:00 - 17:59	IoT Village Hacking Playground	
10:00 - 17:59	Keysight CTF Challenge	
10:00 - 17:59	Living off the Land inside your WiFi : Exploring a . . .	Drew Green,John Rodriguez . . .
10:00 - 17:59	Phisherman's Wharf - Phishing for Beginners	
10:00 - 17:59	Safe Hacking	
10:15 - 11:45	IoT Cat Lamp	Kody K
10:00 - 17:59	IoT Security at DEF CON 32	
10:00 - 17:59	Inside the Toolkit of Elite Embedded Security Expe . . .	
10:00 - 17:59	Firmware Extraction and Analysis	
10:00 - 17:59	Hands-On Hardware Hacking – From Console to Root . . .	
10:00 - 17:59	Hack My TV	
10:00 - 17:59	Hardware Hacking GE Appliances	
12:00 - 13:30	Learn Beginner Soldering With the Meow Mixer Badge	Kody K
13:00 - 13:30	Preparing for the Future: A Discussion of our Rapi . . .	Jamie Hardy,Rachael Tubbs . . .
14:30 - 15:30	Exploration of Cellular Based IoT Technology	Carlota Bindner,Deral Hei . . .
14:00 - 15:59	Solder your own cat shaped WiFi Haking tool	Kody K
15:30 - 15:59	Microhard? More like MicroEASY...to exploit...	Ricky "HeadlessZeke" Laws . . .
15:50 - 16:30	Where’s the Money: Defeating ATM Disk Encryption	Matt Burch
16:30 - 17:59	Meshtastic Meetup	Kody K
17:00 - 17:30	Beyond Sunset: Exposing the Occultations Lurking i . . .	Alexandru Lazar,Dan Berte
17:30 - 17:59	Inside Dash Cam: Custom Protocols and Discovered 0 . . .	Hyo Jin Lee,Hanryeol Park
Saturday		
10:00 - 10:30	SBOMs the Hard Way: Hacking Bob the Minion	Larry Pesce
10:30 - 11:15	Psychic Paper: Making eink access badges accessibl . . .	Joshua Herman
10:00 - 17:59	IoT Security at DEF CON 32	
10:00 - 17:59	IoT Village Hacking Playground	
10:00 - 17:59	Keysight CTF Challenge	
10:00 - 17:59	Living off the Land inside your WiFi : Exploring a . . .	Drew Green,John Rodriguez . . .

PDT Times	Title	speaker
10:00 - 17:59	Phisherman's Wharf - Phishing for Beginners	
10:00 - 17:59	Safe Hacking	
10:15 - 11:45	Learn BadUSB Hacking With the USB Nugget	Kody K
10:00 - 17:59	Hardware Hacking GE Appliances	
10:00 - 17:59	Inside the Toolkit of Elite Embedded Security Expe . . .	
10:00 - 17:59	Hack My TV	
10:00 - 17:59	Firmware Extraction and Analysis	
10:00 - 17:59	Hands-On Hardware Hacking – From Console to Root . . .	
11:15 - 11:59	What To Expect When You're Exploiting: Attacking . . .	Eric Forte,Mark Mager
12:00 - 13:59	LoRa for Hackers : Long Range Hacking for Beginner . . .	Kody K
14:15 - 16:15	Wi-Fi Hacking Self Defense: Four Advanced Techniqu . . .	Kody K
16:30 - 17:59	Meshtastic Meetup	Kody K
Sunday		
10:00 - 12:59	IoT Security at DEF CON 32	
10:00 - 12:59	Safe Hacking	
10:00 - 12:59	Phisherman's Wharf - Phishing for Beginners	
10:00 - 12:59	IoT Village Hacking Playground	
10:15 - 11:45	Wi-Fi Hacker Hunting	Kody K
10:00 - 12:59	Keysight CTF Challenge	
10:00 - 12:59	Living off the Land inside your WiFi : Exploring a . . .	Drew Green,John Rodriguez . . .
10:00 - 12:59	Hack My TV	
10:00 - 12:59	Inside the Toolkit of Elite Embedded Security Expe . . .	
10:00 - 12:59	Hardware Hacking GE Appliances	
10:00 - 12:59	Hands-On Hardware Hacking – From Console to Root . . .	
10:00 - 12:59	Firmware Extraction and Analysis	
12:00 - 12:59	Anyone can hack IoT - a beginner's guide to hack . . .	Andrew "DigitalAndrew" Be . . .
12:00 - 13:30	IoT Cat Lamp	Kody K
12:30 - 12:59	Finding 0days in Vilo Home Routers	Ava Petersen,Justin Mott

Return to Index

LPV - Lock Pick Village

Location: LVCC West/Floor 1/Hall 2/HW2-07-03-A - Map
Home Page: https://www.toool.us/
Sched Page: https://x.com/toool/status/1821662290296660451
DC Discord Chan: https://discord.com/channels/708208267699945503/732734164780056708

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Lockpicking Activities	
12:00 - 12:59	Safecracking for Everyone	Jared Dygert
13:00 - 15:59	Safecracking Practical Demonstration	Jared Dygert
13:30 - 13:59	Doors, Cameras, & Mantraps: Oh my!	Dylan "The Magician" Bakl . . .
Saturday		
10:00 - 17:59	Lockpicking Activities	
12:00 - 14:59	Dozier Drill Tournament	
13:00 - 13:30	Locksport Competitions: Compete in the Olympics of . . .	Matt Burrough
Sunday		
10:00 - 12:59	Lockpicking Activities	

Return to Index

MISC - Misc

Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_MISC

PDT Times	Title	speaker
Wednesday		
00:00 - 00:59	Important Message	
11:00 - 11:59	The Unofficial DEF CON Shoot	
17:00 - 05:59	Linecon	
Thursday		
05:00 - 07:59	Defcon.run	
07:00 - 01:59	Lost & Found	
08:00 - 19:59	Human Registration Open	
08:00 - 17:59	Merch (formerly swag) Area Open -- README	
15:00 - 20:59	Toxic BBQ	
Friday		
05:00 - 07:59	Defcon.run	
06:00 - 06:59	CycleOverride DEF CON Bike Ride	
08:00 - 19:59	Human Registration Open	
08:00 - 17:59	Merch (formerly swag) Area Open -- README	
08:00 - 01:59	Lost & Found	
08:15 - 10:30	ISSCON	
10:00 - 17:59	Vendors and Exhibitors Open	
10:00 - 17:59	All content areas generally open	
10:00 - 17:59	Hard Hat Brigade - Community Space Open	
10:00 - 17:59	Hardware Hacking and Soldering Skills Village Open . . .	
10:00 - 17:59	Robo Sumo	
10:00 - 17:59	HHV Rube Goldberg Machine	
10:00 - 17:59	WISP Community & Inclusion Room	
10:00 - 10:59	Welcome / Badge & Swag Pick Up	
10:00 - 17:59	Game Hacking Community Activities & CTF	
10:00 - 17:59	Shell On Demand Appliance Machine (S.O.D.A. Machin . . .	
10:00 - 15:59	Retro Repair	
10:00 - 15:59	Dumb Terminal fun	
10:00 - 15:59	Small scale LAN party	
10:00 - 15:59	Show & Tell	
10:00 - 17:59	LHC Meshtastic Activities and CTF	
10:00 - 17:59	Egor's Keyboard Corner	
10:00 - 12:59	Resume Reviews	
10:00 - 17:59	Lonely Hackers Club Community Room Open	
10:00 - 17:59	LHC's Unofficial Sticker Swap Table	
10:00 - 10:59	Be Latino in Cybersecurity on markets outside LATA . . .	Salvador Mendonza,Lenin A . . .

PDT Times	Title	speaker
10:00 - 17:59	Open Events for DCNextGen	
11:00 - 11:59	Intro to Circuit Python (Badge class level 1)	
11:30 - 17:30	Book Signings	
11:00 - 11:59	Prendendo Fraudadores utilizando Técnicas de Red . . .	Gustavo Roberto
12:00 - 12:45	Bridging the Gap: How the American Legion Provides . . .	Chris Davis
12:00 - 12:30	SQLi to Root Access: Exploiting a ISP infrastructu . . .	Ignacio Daniel Navarro
12:30 - 13:30	Mexicans Together - Un vistazo a recientes investi . . .	Ashley Hiram M.,Isabel Ma . . .
13:00 - 13:45	No CTF? No Problem! Leveraging Alternate Reality G . . .	John "2PAC" Smithberger
13:30 - 13:59	De Escudo a Espada: Cómo un Antivirus Facilitó e . . .	R4v3n Bl4ck
14:00 - 14:59	Hard Hat Brigade Maker Panel	
14:00 - 15:59	Friendship Bracelet Making	
14:00 - 14:59	Hack the Badge (Badge class level 2)	
14:00 - 17:59	Resume Reviews	
14:00 - 14:45	Book Signing: Visual Threat Intelligence: An Illus . . .	Thomas Roccia
14:00 - 14:59	Amenaza persistente: UXHIL y la propagación de UR . . .	Jesika Juarez,Armando Agu . . .
15:00 - 17:59	C2Society / DC702 Intro to CTFs	
15:00 - 15:45	Generative AI vs Crusty NCO	Col Travis Hartman
15:00 - 15:59	Removing OPSEC from Cyber Predators and Threat Act . . .	Thiago Bordini
16:30 - 17:30	So you wanna know how to make badges	c0ldbru
16:00 - 17:59	Name the Noob	
16:00 - 16:30	Structural Insights: PDF Analysis for Detecting an . . .	Filipi Pires
16:30 - 16:59	Chatbots for Cybersecurity	Lenin Alevski
17:00 - 17:59	Cybersecurity Overview over LATAM- Skills, Challe . . .	Leonardo Pigñer,Katherin . . .
17:30 - 21:30	Ask the EFF	
20:00 - 23:59	DEF CON Movie Night	
21:00 - 01:59	Capitol Technology University (CTU)	
Saturday		
05:00 - 07:59	Defcon.run	
08:00 - 18:59	Human Registration Open	
08:00 - 01:59	Lost & Found	
09:00 - 14:59	Merch (formerly swag) Area Open -- README	
10:00 - 17:59	All content areas generally open	
10:00 - 17:59	Vendors and Exhibitors Open	
10:00 - 17:59	Hard Hat Brigade - Community Space Open	
10:00 - 17:59	HHV Rube Goldberg Machine	
10:00 - 17:59	Robo Sumo	
10:00 - 17:59	Hardware Hacking and Soldering Skills Village Open . . .	
10:00 - 17:59	WISP Community & Inclusion Room	
10:00 - 10:59	Intro to Circuit Python (Badge class level 1) (Ove . . .	
10:00 - 17:59	Game Hacking Community Activities & CTF	
10:00 - 17:59	Shell On Demand Appliance Machine (S.O.D.A. Machin . . .	
10:00 - 15:59	Show & Tell	
10:00 - 15:59	Retro Repair	

PDT Times	Title	speaker
10:00 - 15:59	Dumb Terminal fun	
10:00 - 15:59	Small scale LAN party	
10:00 - 17:59	LHC Meshtastic Activities and CTF	
10:00 - 17:59	Egor's Keyboard Corner	
10:00 - 12:59	Resume Reviews	
10:00 - 17:59	Lonely Hackers Club Community Room Open	
10:00 - 17:59	LHC's Unofficial Sticker Swap Table	
10:30 - 11:30	Protecting the Backbone of Our Modern World	Soledad Antelada Toledano
10:00 - 10:30	Case Study: Hacking Smart Lock For Fun and Profit	Cesar Ortega Ortega
10:00 - 17:59	Open Events for DCNextGen	
11:00 - 11:59	Hack the Badge (Badge class level 2) (Overflow if . . .	
11:30 - 12:30	Cybersecurity for Emerging Tech (panelists would i . . .	Paulino Calderon
12:00 - 12:59	Austin School For The Driven	
12:00 - 12:45	3D Printing My Way to Sanity: The Self-Funding Hob . . .	Steve Dossey
12:30 - 13:30	Threats in Space: The Dangerous Rise of GNSS Attac . . .	Isabel Manjarrez
13:30 - 14:15	How we built our REDACTED THING this year, 5n4ck3y . . .	AND!XOR
13:00 - 13:45	Don't go too far… your job is not done!	Chris Cleary
13:30 - 14:30	DarkGate: Cazando a la amenaza y exponiendo su inf . . .	Nestor Sánchez
14:00 - 14:59	Color Blasted Badge Making: How Hard Could It Be ?	Abhinav Panda,Bradán Lan . . .
14:00 - 14:59	Hard Hat Brigade - Q&A Panel	
14:00 - 15:45	Friendship Bracelet Making	
14:00 - 15:59	DC Book Club Discussion	
14:00 - 17:59	Resume Reviews	
14:00 - 14:45	Navigating Bureaucracy: Strategies for a Post-Mili . . .	Nia Luckey
14:30 - 14:59	Make all the things - Construa seus próprios "bri . . .	Christiane Borges Santos
15:45 - 15:59	WISP Group Photo	
15:00 - 17:59	Name the Noob	
15:00 - 15:45	Cybersecurity for Veterans: Bridging the Gap from . . .	Matt James
15:00 - 15:30	Ransomware B-Sides: Los ransoms que nunca triunfar . . .	Mauro Eldritch,Cybelle Ol . . .
15:30 - 16:30	Haciendo visible lo invisible: Observabilidad y tr . . .	Gastón Aznarez,Octavio G . . .
16:00 - 17:59	Peer-to-Peer Mentoring and Networking with optiona . . .	
16:30 - 17:59	How is GenIA Impacting Cybersecurity: The good, Th . . .	Marco Figueroa
18:30 - 21:30	EFF Tech Trivia	
20:00 - 23:59	DEF CON Movie Night	
21:00 - 01:59	Intigriti Hack Shack	
Sunday		
05:00 - 07:59	Defcon.run	
08:00 - 15:59	Human Registration Open	
08:00 - 14:59	Lost & Found	
10:00 - 12:59	All content areas generally open	
10:00 - 12:59	Vendors and Exhibitors Open	
10:00 - 12:59	Hard Hat Brigade - Community Space Open	
10:00 - 12:59	Robo Sumo	

PDT Times	Title	speaker
10:00 - 12:59	HHV Rube Goldberg Machine	
10:00 - 12:59	Hardware Hacking and Soldering Skills Village Open . . .	
10:00 - 12:59	WISP Community & Inclusion Room	
10:00 - 10:59	Secure From Scatch	
10:00 - 10:59	Game Hacking Community Activities & CTF	
10:00 - 12:59	Shell On Demand Appliance Machine (S.O.D.A. Machin . . .	
10:00 - 12:59	Dumb Terminal fun	
10:00 - 12:59	Retro Repair	
10:00 - 12:59	Small scale LAN party	
10:00 - 12:59	Show & Tell	
10:00 - 12:59	LHC Meshtastic Activities and CTF	
10:00 - 11:59	Egor's Keyboard Corner	
10:00 - 12:59	Lonely Hackers Club Community Room Open	
10:00 - 11:59	LHC's Unofficial Sticker Swap Table	
10:00 - 10:59	Threat Hunting + Intelligence, capabilities, skill . . .	Thiago Bordini,Mauro Eldr . . .
10:00 - 12:59	Open Events for DCNextGen	
11:00 - 11:59	Detección de Vulnerabilidades mediante Instrument . . .	Asher Davila
12:00 - 12:59	Hard Hat Brigade - Group Photo and People's Choice . . .	
12:00 - 12:59	DCNextGen Awards and Closing Ceremony	
12:00 - 12:59	Game Hacking Community Closing Talk & Awards Cerem . . .	
12:00 - 12:59	Abusando de Bitlocker para secuestrar información . . .	Eduardo Chavarro Ovalle
13:00 - 13:59	Jeitinho Cibernético: A Convergência da Seguran. . .	Ueric Melo

Return to Index

PHV - Packet Hacking Village

Location: LVCC West/Floor 2/W216-W221 - Map
Home Page: https://www.wallofsheep.com/
Sched Page: https://www.wallofsheep.com/pages/dc32
DC Discord Chan: https://discord.com/channels/708208267699945503/708242376883306526

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Regular Expressions (RegEx) Trainer	
10:00 - 17:59	FleetDm	
10:00 - 17:59	Password lab	
10:00 - 17:59	Packet Inspector	
10:00 - 17:59	Packet Detective	
10:00 - 17:59	Botnets	
10:00 - 17:59	Linux Trainer	
10:00 - 17:59	Network-OS: Be The Cloud	
10:00 - 17:59	Python + Packet Analysis + Machine Learning	
12:00 - 12:59	The Curious Case of Alice and Bob: What You Can (A . . .	Catherine J. Ullman
13:00 - 13:30	MoWireless MoProblems: Modular Wireless Survey Sys . . .	Geoff Horvath,Winson Tam
13:30 - 14:30	Signature-Based Detection Using Network Timing	Josh Pyorre
Saturday		
10:00 - 17:59	Python + Packet Analysis + Machine Learning	
10:00 - 17:59	Packet Inspector	
10:00 - 17:59	FleetDm	
10:00 - 17:59	Packet Detective	
10:00 - 17:59	Botnets	
10:00 - 17:59	Password lab	
10:00 - 17:59	Linux Trainer	
10:00 - 17:59	Network-OS: Be The Cloud	
10:00 - 17:59	Regular Expressions (RegEx) Trainer	
10:00 - 10:59	Using AI Computer Vision in Your OSINT Data Analys . . .	Mike Raggo
11:00 - 11:30	Introduction to IPv6	Denis Smajlović
16:30 - 16:59	Decoding Galah, an LLM Powered Web Honeypot	Adel Karimi
17:00 - 17:59	Exposing Coordinated Attacks Hiding in the Sheer N . . .	Ezz Tahoun,Lynn Hamida
Sunday		
10:00 - 13:59	Python + Packet Analysis + Machine Learning	
10:00 - 13:59	Regular Expressions (RegEx) Trainer	
10:00 - 13:59	Network-OS: Be The Cloud	
10:00 - 13:59	Linux Trainer	
10:00 - 13:59	Botnets	
10:00 - 13:59	Packet Detective	
10:00 - 13:59	FleetDm	

PDT Times	Title	speaker
10:00 - 13:59	Password lab	
10:00 - 13:59	Packet Inspector	
12:00 - 12:59	Winning the Game of Active Directory	Brandon Colley

Return to Index

PLV - Policy Village

Location: LVCC West/Floor 2/W237 - Map
Home Page: https://defcon.org/policy/

PDT Times	Title	speaker
Friday		
10:00 - 11:45	US and International Public Cyber Policy 101	Harley Geiger,Adam Dobell . . .
12:00 - 12:45	Rules All Hackers Must Follow in War	Dr. Kosuke Onishi
13:00 - 13:45	The Value of Trust in the Open-source Software Eco . . .	Nasreen Djouini,Jordan Ka . . .
14:30 - 15:15	Human Dignity in AI and Tech Policy	Jan Trzaskowski
14:00 - 14:45	Advocating for an Inclusive Cyber-Civil Rights Pol . . .	Nicole Tisdale,Kemba Wald . . .
15:15 - 15:59	Open Source Hacker Vs. Government Lawyer: Clashing . . .	Eddie Zaneski,Rebecca Liv . . .
15:00 - 16:45	NSM-22 and the National Risk Management Plan: CISA . . .	William Loomis,Michael Ga . . .
16:00 - 16:30	Cybersecurity Schoolhouse Rock	Avi McGrady
17:00 - 17:45	Singapore - Safeguarding the Nation: The Vital Rol . . .	NG Yeow Boon,Bill Woodcoc . . .
Saturday		
11:00 - 12:20	How can hackers support efforts to secure AI syste . . .	Wan Ding Yao,Christine La . . .
12:30 - 13:15	Pick Your Poison: Navigating a secure clean energy . . .	Emma Stewart
12:30 - 12:50	Measuring the international balance of trade in In . . .	Bill Woodcock
13:15 - 13:59	Hacker vs AI: perspectives from an ex-spy	Harriet Farlow
13:00 - 13:45	Global Perspectives in Cybersecurity: Challenging . . .	Wouter Veenstra,Randy Pes . . .
14:00 - 15:45	What's next for the commercial CNE marketplace? . . .	UK Repersentative 2,Senio . . .
17:00 - 17:45	Challenges and Reactions: Cybersecurity and Commun . . .	Herming Chiueh
Sunday		
11:00 - 11:45	Flying Blind: Navigating the Turbulent Skies of Av . . .	Mike Weigand,Stuart Wagne . . .

Return to Index

PSV - Physical Security Village

Location: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map
Home Page: https://www.physsec.org/
DC Discord Chan: https://discord.com/channels/708208267699945503/732732893830447175

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Physical Security Village Activities	
12:30 - 12:59	RFID 101	Andrew M,Ege Feyzioglu
12:00 - 12:59	Flipping Locks (The Remix) - Remote Badge Cloning . . .	Langston Clement,Dan Goga
13:00 - 13:59	Bypass 101	Karen Ng,Sam Mayers
13:30 - 13:59	Bogus Badges: The Art and Innovation of Badge Coun . . .	Nick Warner
14:00 - 14:30	Physical Security Assessment Basics for Internal E . . .	Billy Graydon
14:30 - 15:30	Your Smartcard is Dumb: A Brief History of Hacking . . .	Chad Shortman
16:00 - 16:30	Access Control done right the first time	Tim Clevenger
17:00 - 17:59	Bypass 101	Karen Ng
Saturday		
10:00 - 17:59	Physical Security Village Activities	
11:00 - 12:59	Social Engineering Improv Acting Techniques	Tim Roberts
13:00 - 13:30	Smart Shopping Cart Wheels - How they Work	Joseph
14:00 - 14:59	HandPwning: “Your Hand is your Passport. Verify . . .	Luca "CYBERANTANI" Bongio . . .
15:30 - 15:59	Access Control Done Right the First Time	Tim Clevenger
15:00 - 15:30	Bypass 102	Karen Ng,Terry Luan
15:30 - 16:30	Intermediate Physical Security	Justin Wynn
17:00 - 17:59	Flipping Locks (The Remix) - Remote Badge Cloning . . .	Langston Clement,Dan Goga
Sunday		
10:30 - 11:30	Bypass 101	Karen Ng
10:00 - 12:59	Physical Security Village Activities	
11:00 - 11:30	Physical OSINT	Lukas McCullough
11:30 - 11:59	Fitness of Physical Red Teamers	Billy Graydon,Lucas Rooya . . .
11:30 - 11:59	HandPwning: “Your Hand is your Passport. Verify . . .	Luca "CYBERANTANI" Bongio . . .

Return to Index

PYV - Payment Village

Location: LVCC West/Floor 2/W202 - Map
Home Page: https://www.paymentvillage.org/
Sched Page: https://www.paymentvillage.org/workshops
DC Discord Chan: https://discord.com/channels/708208267699945503/732733473558626314

PDT Times	Title	speaker
Friday		
10:00 - 16:30	Payment Village CTF	
10:15 - 10:20	Introduction to Payment Village CTF	Leigh-Anne Galloway
11:30 - 12:40	User Behaviour Analytics in Payments	Karthik Tadinada
13:00 - 13:59	Attacking and defending card present transactions	Yurii Zadoianchuk,Stephan . . .
14:30 - 15:10	Emulating Magstripe with Arduino	Leigh-Anne Galloway
16:30 - 16:59	Payment Village CTF Day One Results	
Saturday		
10:00 - 16:30	Payment Village CTF	
10:45 - 10:59	Introduction to the Payment Village badge	Leigh-Anne Galloway
10:15 - 10:20	Introduction to Payment Village CTF	Leigh-Anne Galloway
11:30 - 12:10	Emulating Magstripe with Arduino	Leigh-Anne Galloway
13:00 - 13:59	Breaking software protected crypto implementations	Adrian Garcia
15:00 - 15:59	Online Payments - Attack and Defense	Vincent Sloan
16:30 - 16:59	Payment Village CTF Day Two Results	

Return to Index

QTV - Quantum Village

Location: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map
Home Page: https://quantumvillage.org/

PDT Times	Title	speaker
Friday		
10:05 - 11:25	Intro to Quantum with Q#	Mariia Mykhailova
10:00 - 10:59	QOLOSSUS: QUANTUM CTF CONTEST: How to get Started . . .	
11:25 - 12:15	How do we make LLVM quantum?	Josh Isaac
12:15 - 12:59	A Hacker's guide to PQC	Konstantinos Karagiannis
14:00 - 14:59	Quantum on the flip side - A global south perspect . . .	Bruna Shinohara de Mendon . . .
15:00 - 15:59	Trapped Ion Quantum Computing Systems - Behind The . . .	Daiwei Zhu,Rick Altherr
16:00 - 16:59	Attack Vectors of Quantum Computers	Sorin Boloș,Adrian Cole. . .
17:00 - 17:30	DevSecOps of Quantum Computers	
17:30 - 17:59	Threat Modelling: Quantum Computers	
Saturday		
10:00 - 10:59	Intro to QKD: Quantum Key Exchange: Beyond the Hyp . . .	Ben Varcoe
11:00 - 11:59	Hacking Quantum Key Distribution (QKD)	Vadim Makarov
12:00 - 12:59	Threat Modelling QKD	
14:00 - 14:45	QML - Quantum Machine Learning: What is it, where . . .	Josh Izaac
14:45 - 15:30	Playing with Quantum: wayfinding with quantum game . . .	Michael Dascal
15:30 - 16:30	Covert Quantum Communication	Evan Anderson
16:30 - 17:29	The Quantum Ethics and Skills Debates	Bob Gourley,Bruna Shinoha . . .
16:30 - 17:59	Quantum Village Bloch Party!	
17:15 - 17:59	Bloch Party & More Debates	
Sunday		
10:00 - 10:59	Physical Fundamentals of Quantum Computing	Erez M Abrams
11:00 - 11:59	FIDO2 in the Quantum Realm	Nina Bindel,James Howe
12:00 - 12:59	Policy and the Quantum: Where do we start?	
13:15 - 14:14	QOLOSSUS CONTEST Q-CTF Finals	

Return to Index

RCV - Recon Village

Location: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map
Home Page: https://www.reconvillage.org/
Sched Page: https://www.reconvillage.org/talks
DC Discord Chan: https://discord.com/channels/708208267699945503/732733566051418193

PDT Times	Title	speaker
Friday		
10:45 - 11:30	Recursion is a Harsh Mistress: How (Not) To Build . . .	TheTechromancer
10:00 - 13:59	Recon Village GE(O)SINT Challenge	
10:00 - 10:45	Bastardo Grande: Hunting the Largest Black Market . . .	Bryan Hance
11:30 - 12:05	Hospitals, Airports, and Telcos — Modern Approac . . .	Itay Cohen
12:40 - 13:25	SWGRecon: Automate SWG Rules, Policy, and Bypass E . . .	Vivek Ramachandran
12:05 - 12:40	Bypassing WHOIS Rate Limiting and Alerting on Fres . . .	Willis Vandevanter
12:00 - 12:59	Ask Me Anything - Daniel Cutberth, Moderated by Su . . .	Sudhanshu,Daniel Cuthbert
13:25 - 13:59	Tapping the OSINT potential of Telegram	Megan Squire
13:00 - 13:59	Interview - Mika Devonshire, Hosted by Himanshu Da . . .	Mika Devonshire,Himanshu . . .
14:00 - 17:59	ToolMakers Hackathon	
15:45 - 16:20	Recon MindMap: Organize, Visualize, and Prioritize . . .	Lenin Alevski
15:00 - 15:59	Interview - Scott Helme, Hosted by Shubham	Scott Helme,Shubham
15:00 - 15:45	GeoINT Mastery: A pixel is worth a thousand words	Mishaal Khan
16:00 - 16:59	Interview - the gumshoo, Hosted by Ram	the gumshoo,Ram
17:45 - 18:15	OSINT at Clemson: Unmasking John Mark Dougan's Dis . . .	Steven Sheffield
17:05 - 17:45	Pushing the limits of mass DNS scanning	Jasper Insinger
Saturday		
10:00 - 11:59	Maltego Community Workshop	Carlos Fragoso
10:00 - 10:59	Interview - CATO Networks, Hosted by Dhruv Shah	CATO Networks,Dhruv Shah
10:00 - 13:59	Recon Village GE(O)SINT Challenge	
11:00 - 11:59	Interview - RedHunt Labs (Kunal), Hosted by Anant . . .	RedHunt Labs (Kunal),Anan . . .
12:00 - 13:59	OWASP Amass Expanding Data Horizons: Amassing More . . .	Jeff Foley
12:00 - 12:59	Interview - Daniel Miessler, Hosted by Ankur	Daniel Miessler,Ankur
14:00 - 17:59	ToolMakers Hackathon	
14:00 - 15:59	The art of Pivoting in OSINT Investigations	Ram Ganesh

Return to Index

RFV - Radio Frequency Village

Location: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map
Home Page: https://rfhackers.com/
DC Discord Chan: https://discord.com/channels/708208267699945503/732732595493666826

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Radio Frequency Village Events	
10:30 - 11:25	RF CTF Kick Off Day 1	RF Hackers
11:30 - 12:25	Software Defined Radio 101: Capturing Your First R . . .	bkobe
12:30 - 13:25	Exploiting insecure OTA updates to create the worl . . .	Lozaning
13:30 - 14:25	iCLASS - Throwing away the keys	Tiernan "nvx" Messmer
14:30 - 15:25	Yet another way of exfiltrating data from air-gapp . . .	C$,Endeavors
15:30 - 15:55	Warwheeling: The Wireless Sk8r	r1otctrl
16:00 - 16:25	A Short Introduction to 802.11ah Long Range WiFi H . . .	Ronald Broberg,Robert Van . . .
16:30 - 17:25	Meshtastic Adventures: Triumphs, Tribulations, and . . .	m1ddl3w4r3
Saturday		
10:30 - 11:25	RF CTF Kick Off Day 2	RF Hackers
10:00 - 17:59	Radio Frequency Village Events	
11:30 - 12:30	AMA on Proxmark3 with Iceman	Iceman
12:30 - 12:55	DoorSim - making my conference travel easier	evildaemond (Adam Foster)
13:00 - 13:59	Exploring the Cosmos: Hackable Innovations at the . . .	Luigi Cruz
14:00 - 14:59	Remote Sensor Node Updates for FISSURE - The RF Fr . . .	Chris Poore
15:30 - 15:55	Who's Afraid of Synthetic Aperture Radar?	Abraxas3d
15:00 - 15:25	Current EW techniques	Kent Britain
16:00 - 16:50	Tracking Real-Time Locations with Rogue WiFi Packe . . .	Mikey Awbrey
Sunday		
10:00 - 12:59	Radio Frequency Village Events	
12:30 - 12:59	World Wide War Drive Outbrief	RF Hackers,WiGLE Staff

Return to Index

RTV - Red Team Village

Location: LVCC West/Floor 2/W204-W207 - Map
Home Page: https://redteamvillage.io/
Sched Page: https://redteamvillage.io/schedule.html

PDT Times	Title	speaker
Friday		
11:00 - 11:50	The Art of Critical Thinking through an Adversaria . . .	Ben "NahamSec" Sadeghipou . . .
12:00 - 12:50	Mining for Abandoned Gold in DNS	Matt Pawloski
12:00 - 12:50	Modern Red Teaming: macOS, K8s, and Cloud	Chris Gates,int eighty (o . . .
12:00 - 12:50	Abusing DevOps to Pivot Between Cloud and On-Prem	Colbert Zhu,Tom Porter
12:00 - 12:50	Red Team Terraform Workshop	Moses Frost
12:00 - 12:50	Bypassing Corporate controls on Mac Devices	Adwiteeya Agrawal,Ian Fos . . .
13:00 - 16:59	DC NextGen / Youth Challenge Area at Red Team Vill . . .	RTV Staff
13:00 - 13:50	Red Goes Purple: Executing the Attack Path	Omar Santos,Graham Helton . . .
13:00 - 13:50	Adversary Simulation: Using Blue Eyes to See Red	Fred Wilmot,Sebastien Tri . . .
13:00 - 13:50	Simulated Drone Hacking	Nick Aleks
13:00 - 14:50	Badge Cloning: A Penetration Tester's Guide to Ca . . .	Travis Weathers,Ralph May
14:00 - 14:50	Physical Security - Bypassing Access Control Syste . . .	Andrew Johnson
14:00 - 14:50	Level UP OSINT	Mishaal Khan
14:00 - 15:50	Modifying Impacket for Better OpSec	Ryan O'Donnell
15:00 - 15:50	Threat Emulation 101	Trey Bilbrey
15:00 - 16:50	New Skill Unlocked: C2 Infrastructure Automation	Josh Huff,Robert Pimentel
15:00 - 15:50	GHOST in the Model: Generating AI-Assisted Threat . . .	Sam Cosentino
16:00 - 16:50	Mac-n-Cheese: How to Cook Up Delicious Electron Te . . .	Roberto Soares
16:00 - 16:50	Thinking Outside the Kube - Finding and Exploiting . . .	Tomer Peled
16:00 - 16:50	Building Your Red-Teaming Co-Pilot: Navigating the . . .	Gaspard Baye
16:00 - 16:59	Blue Goes Purple: Purple Teams for Fun and Profit . . .	Catherine J. Ullman,Jake . . .
Saturday		
10:00 - 10:50	The Hybrid Horizon: Unleashing the Power of Azure . . .	Chirag Savla,Raunak Parma . . .
10:00 - 10:50	BOAZ, Yet Another layered Evasion Tool: Unveiling . . .	Thomas X Meng
10:00 - 10:50	DoH Deception: Evading ML-Based Tunnel Detection w . . .	Emanuel Valente
10:00 - 10:50	Physical Red Teaming for Offensive Cyber Teams	Shawn Abelson,Ana Aslanis . . .
10:00 - 10:50	Hacking the Skies – Satellite Red Teaming	Agostino Panico
11:00 - 11:50	OSINT for Hackers	Lee McWhorter,Sandra Stib . . .
11:00 - 11:50	Securing the Future with CoSAI: Identified Technic . . .	Omar Santos,Dan McInerney . . .
11:00 - 11:50	Developing Evilginx Phishlets	Michael Donley
11:00 - 11:50	RustOps	Jose Plascencia
11:00 - 11:50	Island Hoping: Move from LOLBins to Living off Lan . . .	Moses Frost
12:00 - 16:59	DC NextGen / Youth Challenge Area at Red Team Vill . . .	RTV Staff
12:00 - 12:50	Insert coin: Hacking arcades for fun	Ignacio Daniel Navarro
12:00 - 12:50	Developing Better Payloads with Automated Testing	Nick McClendon

PDT Times	Title	speaker
12:00 - 12:50	Tunnel Vision: Exploring VPN Post-Exploitation Tec . . .	Ori David
13:00 - 14:50	An Operator's Guide: Hunting SCCM in the Real Worl . . .	Garrett Foster,Zachary St . . .
13:00 - 13:50	macOS Red Team on Corporate Scenarios	Ricardo L0gan
13:00 - 13:50	Building Surgical Implants: A Comprehensive Guide . . .	John Rodriguez
14:00 - 14:50	Cloud Offensive Breaches: The Graph-Based Exploita . . .	Filipi Pires
14:00 - 14:50	Tempest c2: Use and Design	Kirk Trychel
14:00 - 14:50	Combining Uncensored and Censored LLMs for Ransomw . . .	Muhammad Mudassar Yamin
15:00 - 15:50	The Curious Case of Stealer Logs: Access & Espiona . . .	Eric Clay,Nick Ascoli
15:00 - 15:50	Introduction to Kubernetes common attack technique . . .	Lenin Alevski
15:00 - 15:50	Using Retrieval Augmented Generation (RAG), Langch . . .	Omar Santos
15:00 - 16:59	Learning the New Amass Collection Engine	Jeff Foley
16:00 - 16:50	Pipeline Pandemonium: How to Hijack the Cloud and . . .	Blake Hudson
16:00 - 16:50	Hacking Policy and Policy Hacking - A Red-Teamer H . . .	Amit Elazari
16:00 - 16:50	Bespoke C2s are coming of age.	David "Icer" Maynor
Sunday		
10:00 - 11:50	DC NextGen / Youth Challenge Area at Red Team Vill . . .	RTV Staff
10:00 - 10:50	From Runners to IdP Admin	Sim Cher Boon
10:00 - 10:50	From Network to Network: Hands-On Pivoting Techniq . . .	Francisco Canteli
10:00 - 10:50	IDOR in Financial Operations	Ilkin Javadov
10:00 - 10:50	Hacking Processes: Introducing the Redteaming Proc . . .	Alex Gonzalez,Bobby R
10:00 - 10:59	The Village Peoples' Panel - What Really Goes On i . . .	Justin,Matt Mayes,muteki, . . .
11:00 - 11:50	The SIEMless Hack: Rewriting Reality with Log Inje . . .	Özgün Kültekin
11:00 - 11:50	Threat hunting like a pentester	Ronald Gonzalez
11:00 - 11:50	Red Team Infrastructure Setup and Automation	Aravind Prakash,Arun Nair . . .
11:00 - 11:50	Supercharge your vuln finding workflow with automa . . .	Erik Hunstad,Alberto Rodr . . .

Return to Index

SEV - Social Engineering Village

Location: LVCC West/Floor 3/W317-W319 - Map
Home Page: https://www.se.community/
Sched Page: https://www.se.community/schedule/
DC Discord Chan: https://discord.com/channels/708208267699945503/732733952867172382

PDT Times	Title	speaker
Friday		
08:30 - 17:59	Social Engineering Community Village Hours	
17:15 - 17:59	Presentation: The 2024 #SECVC Debrief	
Saturday		
10:00 - 17:59	Social Engineering Community Village Hours	
10:00 - 12:30	John Henry Competition - Human vs. AI & Panel Disc . . .	
12:30 - 12:59	SECV - Break / Networking	
13:00 - 14:59	Cold Calls	
15:30 - 17:30	Cold Calls	
15:00 - 15:30	SECV - Break / Networking	
17:30 - 17:59	Presentation: It Takes a Village...	
Sunday		
10:00 - 11:30	SECVC Awards & Competitor Panel + Youth Challenge . . .	
10:00 - 13:59	Social Engineering Community Village Hours	
11:30 - 13:59	Cold Calls	

Return to Index

SOC - Social Activities: Parties/Meetups

PDT Times	Title	speaker
Thursday		
12:00 - 12:59	Friends of Bill W	
16:00 - 17:59	QueerCon Mixer	
17:00 - 17:59	Friends of Bill W	
19:00 - 20:59	DC702	
20:00 - 01:59	Music Set / Entertainment (Cyberpunk Bar Thursday, . . .	Talk Sinn,Stitcharoo,Rela . . .
20:00 - 01:59	Music Set / Entertainment (Thursday, SYN Stage)	PatAttack,Grind613,DotOrN . . .
Friday		
12:00 - 12:59	Friends of Bill W	
12:00 - 13:30	Veilid Dev and Community Meetup	
16:00 - 18:59	DEF CON Holland Group Presents: VrijMiBo	
16:00 - 17:59	QueerCon Mixer	
16:00 - 18:59	DCG Atlanta (DC404,678,770,470)	
17:00 - 17:59	Friends of Bill W	
18:30 - 22:30	Policy Mixer @ DEF CON	
19:30 - 21:59	Lawyers Meet	
19:00 - 00:59	BlanketFort Con	
19:00 - 01:59	Blacks in Cyber Lituation 2.0	BIC Village Staff,DJ Roma
20:00 - 01:59	Music Set / Entertainment (Cyberpunk Bar Friday, A . . .	Scotch & Bubbles,PankleDa . . .
20:00 - 01:59	Hacker Karaoke	
20:00 - 01:59	Music Set / Entertainment (Retro Sci-Fi Friday, SY . . .	ZEE,YTCracker,TRIODE,Ohm- . . .
21:00 - 01:59	Arcade Party	
21:00 - 01:59	GOTHCON 2024	
22:00 - 00:59	QueerCon	
Saturday		
12:00 - 12:59	Friends of Bill W	
16:00 - 17:59	QueerCon Mixer	
17:00 - 18:59	Sticker Swap at DEF CON 32	
17:00 - 17:59	Friends of Bill W	
18:30 - 22:30	Policy Mixer @ DEF CON	
19:30 - 21:59	DC Next Gen party	
19:00 - 20:59	Women, gender non-conforming and non-binary meetup . . .	
20:00 - 01:59	Music Set / Entertainment (Cyberpunk Bar Saturday, . . .	Wesley McGrew,Syntax (DJ) . . .
20:00 - 01:59	Hacker Karaoke	
20:00 - 01:59	Music Set / Entertainment (Pirate's Night For Me! . . .	Skittish and Bus,O'Craven . . .
20:00 - 23:59	AIV + BTV Pool Party featuring DUNK-A-FED	
21:00 - 01:59	VETCON	
21:00 - 01:59	The Illuminati Party	

PDT Times	Title	speaker
21:00 - 01:59	RAA for Workgroups 3.11	
21:00 - 00:59	Jack Rhysider Masquerade Party	Jack Rhysider
Sunday		
10:30 - 12:20	WarDriver Meetup	
12:00 - 12:59	Friends of Bill W	

Return to Index

TCV - Telecom Village

Location: LVCC West/Floor 2/W201 - Map
Home Page: https://telecomvillage.com/
Sched Page: https://telecomvillage.com/index.html#program-details

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Telecom Village Inauguration	
11:00 - 13:59	5G Fortress	Akib Sayyed
15:00 - 16:59	Telecom Time Machine	Nadeem Bagwan
17:00 - 17:59	SIMply Secure	Zibran Sayyed
Saturday		
10:00 - 10:59	AI-Driven Cyber Resilience: Surviving the 5G Threa . . .	Shina Liu,Niklas Lindroos . . .
11:00 - 13:59	GPON Unplugged	Akib Sayyed
15:00 - 16:59	4G Frenzy	Vinod Shrimali
Sunday		
10:00 - 13:59	Telecom Tinkerer CTF	

Return to Index

TEV - Tamper Evident Village

Location: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Tamper Evident Village Activities	
Saturday		
10:00 - 17:59	Tamper Evident Village Activities	
Sunday		
10:00 - 12:59	Tamper Evident Village Activities	

Return to Index

VMV - Voting Village

Location: LVCC West/Floor 2/W223-W224 - Map
Home Page: https://votingvillage.org/
DC Discord Chan: https://discord.com/channels/708208267699945503/732733881148506164

PDT Times	Title	speaker
Friday		
10:00 - 10:45	What is the Voting Village?	Catherine Terranova,Matt . . .
10:45 - 11:45	Play by Play of the Curling v. Raffensperger Lawsu . . .	Susan Greenhalgh,Mary Kai . . .
10:00 - 12:59	SIV Internet Voting Hacking Challenge	SIV
11:45 - 12:45	How to Steal Voting Software and Get Away With It	Susan Greenhalgh,Anna Bow . . .
13:00 - 13:59	Risk Limiting Audits From the Source	Philip Stark
14:45 - 15:30	What Does it Mean to be an American?	Kendall Spencer
14:30 - 14:45	Risk Limiting Audit DEMO by Philip Stark	Philip Stark
14:00 - 14:45	Election 2024 Freedom of Choice: A Psybernomic Con . . .	Hallie Stern,Tina Schneib . . .
15:30 - 16:15	Breaking Through Election Myths	Will Baggett
16:15 - 16:59	Maricopa County -Preparing for the 2024 Elections . . .	Nate Young,Jason Butryn
17:00 - 17:45	Hacking the Vote: How Hackers Caused the Downfall . . .	Fleur van Leusden
Saturday		
10:00 - 10:45	Voting Village Opening Remarks	Catherine Terranova,Harri . . .
11:00 - 11:45	Democracy From Around the World	Harri Hursti
11:00 - 11:59	First Time TSX Hacking Challenge	Tailor Tolliver
11:45 - 12:15	The Threat of Deepfakes and Synthetic Media to Ele . . .	Dr. Matthew Canham
12:15 - 13:15	Indivisible	Michael Moore
13:15 - 13:59	Stanford Digital Observatory	Renée DiResta
14:00 - 14:45	Understanding the Role of Secretary of States in E . . .	Dave Scanlan
14:45 - 15:30	Understanding Cognitive Warefare in a Geopolitcal . . .	Constantine Nicolaidis
15:30 - 16:30	Cognative Weather Report	Constantine Nicolaidis,Ca . . .
16:30 - 16:59	What Do Long Voter Registration Lines Mean?	Jake Braun
17:00 - 17:45	Misinformation, Disinformation, and Malformation i . . .	Nicole Tisdale,Michael Mo . . .

Return to Index

WS - DEF CON Workshops

Home Page: https://defcon.org/html/defcon-32/dc-32-workshops.html
Sched Page: https://defcon.outel.org/defcon32/dc32-consolidated_page.html#villist_WS

PDT Times	Title	speaker
Thursday		
09:00 - 12:59	Sold Out - Offensive SCCM: Abusing Microsoft's C2 . . .	Chris Thompson,Duane Mich . . .
09:00 - 12:59	Sold Out - Med Team vs Red Team: Intro into Medica . . .	Alex Delifer,Michael "v3g . . .
09:00 - 12:59	Sold Out - Supercharge SAST: Semgrep Strategies fo . . .	Arjun Gopalakrishna,Gauta . . .
09:00 - 12:59	Sold Out - Dissecting Malware for Defense - Crafti . . .	Francisco Perdomo,Josh St . . .
09:00 - 12:59	Sold Out - Tracing The Pain Away - Practical Binar . . .	Sean ,Serrgei Frankoff
14:00 - 17:59	Sold Out - Flipping the Coin: Red and Blue Teaming . . .	Angus Strom,Troy Defty
14:00 - 17:59	Sold Out - Long Live Empire: A C2 Workshop for Mod . . .	Jake “Hubble” Krasnov . . .
14:00 - 17:59	Sold Out - 64-bit Intel Assembly Language Programm . . .	Wesley McGrew
14:00 - 17:59	Sold Out - Dodging the EDR Bullet: A Workshop on M . . .	Dimitri Di Cristofaro,Gio . . .
14:00 - 17:59	Sold Out - Hide your kids, turn off your Wi-Fi, th . . .	James Hawk
Friday		
09:00 - 12:59	Sold Out - Traumatic Library Loading : If you want . . .	Yoann Dequeker
09:00 - 12:59	Sold Out - Finding the Needle: An Introduction to . . .	Kathy Zhu,Troy Defty
09:00 - 12:59	Sold Out - Whitebox Web Exploit Development	Cale Smith,Priyanka Joshi
09:00 - 12:59	Sold Out - Small Choices, Global Repercussions: A . . .	Isabel Straw,Jorge Aceved . . .
09:00 - 12:59	Sold Out - Machine Learning for N00bs	Elizabeth Biddlecome,Irvi . . .
14:00 - 17:59	Sold Out - Ghidra Analysis & Automation Masterclas . . .	Max "Libra" Kersten
14:00 - 17:59	Sold Out - Learning to Hack Bluetooth Low Energy w . . .	Alek Amrani,Ryan Holeman
14:00 - 17:59	Sold Out - Hack the connected plant!	Alexandrine Torrents,Arna . . .
14:00 - 17:59	Sold Out - From an attacker's lair to your home: A . . .	Sebastian Tapia De la tor . . .
14:00 - 17:59	Sold Out - Dissecting and Defeating Ransomware's E . . .	Aaron Rosenmund,Josh Stro . . .
Saturday		
09:00 - 12:59	Sold Out - Sharp Security from All Angles: Masteri . . .	Or Sahar,Yariv Tal
09:00 - 12:59	Sold Out - Hacking The Metal: A Spark of Intellige . . .	eigentourist
09:00 - 12:59	Sold Out - Capture the Flag 101	Micah Silverman
09:00 - 12:59	Sold Out - Hacking Apps on Salesforce	Rodney David Beede
09:00 - 12:59	Sold Out - Industrial Control Systems: how to secu . . .	Alexandrine Torrents
14:00 - 17:59	Sold Out - Email Detection Engineering and Threat . . .	Alfie Champion,Josh Kamdj . . .
14:00 - 17:59	Sold Out - Crash Course in Physical Access Control . . .	Lorenzo Pedroncelli,Randy . . .
14:00 - 17:59	Sold Out - Playing with RFID	Vinnie "kernelpaniek" Van . . .
14:00 - 17:59	Sold Out - Master Class: Hands-On Machine Learning . . .	Solomon Sonya

Return to Index

XRV - XR Village

Location: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map
Home Page: https://xrvillage.org/

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Pwning through the Metaverse - Quest Headset Vulne . . .	Luke McLaren
10:00 - 17:59	Signals Are Everywhere	
10:00 - 17:59	ICS Village + XR Village Turn the lights on!	
11:00 - 11:30	National Labs Use of XR	Martin Pratt
11:00 - 12:59	Trip Through Reality XR for Performances Mastercla . . .	The Glad Scientist
14:00 - 17:59	Extend reality with tabletop RPG OWASP Cornucopia. . . .	Stryker
17:00 - 17:59	Be the Ghost in the Shell Barrier Mazes FTW	David "Icer" Maynor
Saturday		
10:00 - 17:59	Signals Are Everywhere	
10:00 - 17:59	ICS Village + XR Village Turn the lights on!	
11:30 - 11:59	Student Engagement Doesn't Have to Suck	Dr. Muhsinah Morris
11:00 - 12:59	AR + Art = interactive installations to bring your . . .	Zaire Moore
12:00 - 12:30	XR for All: Accessibility and Privacy for Disabled . . .	Dylan Fox
Sunday		
10:00 - 11:59	Play All the Things	
10:00 - 10:30	Evolution of RF Signal Visualization - From Spectr . . .	Suzanne Borders,Jad Meouc . . .

Return to Index

CON - Friday - 10:00-17:59 PDT

Title: ? Cube
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02 - Map

Description:

In-Person Contest Friday and Saturday: 10:00-18:00; Sunday: 10:00-12:00

The Return of ? Cube

? Cube returns, weaving a tale that transcends the ordinary. This year, engagement is not just a theme—it's a journey through the multidimensional realms of hacking. Progressive Puzzles: Unlock the secrets of each compartment as you journey through progressively harder puzzles. From the Front's gentle introduction to the Top's formidable challenges, the Cube invites you to engage with the spectrum of cybersecurity domains. Physical Entry Unleashed: In a bold evolution, physical entry becomes a key component. Navigate the tangible aspects of physical entry, decoding not only in the digital realm but also as you immerse yourself physically in the enigmatic sides of ? Cube. Cryptic Narratives: As each compartment unfolds, the narrative of engagement takes shape. The puzzles, touching on encryption, penetration testing, and beyond. Silent Intricacies: Engage not only with the puzzles but also with the silent intricacies woven into the physical challenges. Decrypt messages, decipher patterns, and embrace the essence of Defcon as you navigate the unseen and the tangible. Embark on the Engage Journey: ? Cube calls upon the curious and the bold. Embark on a journey where the puzzles transcend the digital divide, demanding both mental acuity and physical prowess.
H4QEG5LCMUQEAICEMVTGG33OEAZTEICSMVQWI6JAORXSAZLOM5QWOZJ7

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: ? Cube
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02 - Map

Description:

In-Person Contest Friday and Saturday: 10:00-18:00; Sunday: 10:00-12:00

The Return of ? Cube

? Cube returns, weaving a tale that transcends the ordinary. This year, engagement is not just a theme—it's a journey through the multidimensional realms of hacking. Progressive Puzzles: Unlock the secrets of each compartment as you journey through progressively harder puzzles. From the Front's gentle introduction to the Top's formidable challenges, the Cube invites you to engage with the spectrum of cybersecurity domains. Physical Entry Unleashed: In a bold evolution, physical entry becomes a key component. Navigate the tangible aspects of physical entry, decoding not only in the digital realm but also as you immerse yourself physically in the enigmatic sides of ? Cube. Cryptic Narratives: As each compartment unfolds, the narrative of engagement takes shape. The puzzles, touching on encryption, penetration testing, and beyond. Silent Intricacies: Engage not only with the puzzles but also with the silent intricacies woven into the physical challenges. Decrypt messages, decipher patterns, and embrace the essence of Defcon as you navigate the unseen and the tangible. Embark on the Engage Journey: ? Cube calls upon the curious and the bold. Embark on a journey where the puzzles transcend the digital divide, demanding both mental acuity and physical prowess.
H4QEG5LCMUQEAICEMVTGG33OEAZTEICSMVQWI6JAORXSAZLOM5QWOZJ7

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: ? Cube
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02 - Map

Description:

In-Person Contest Friday and Saturday: 10:00-18:00; Sunday: 10:00-12:00

The Return of ? Cube

? Cube returns, weaving a tale that transcends the ordinary. This year, engagement is not just a theme—it's a journey through the multidimensional realms of hacking. Progressive Puzzles: Unlock the secrets of each compartment as you journey through progressively harder puzzles. From the Front's gentle introduction to the Top's formidable challenges, the Cube invites you to engage with the spectrum of cybersecurity domains. Physical Entry Unleashed: In a bold evolution, physical entry becomes a key component. Navigate the tangible aspects of physical entry, decoding not only in the digital realm but also as you immerse yourself physically in the enigmatic sides of ? Cube. Cryptic Narratives: As each compartment unfolds, the narrative of engagement takes shape. The puzzles, touching on encryption, penetration testing, and beyond. Silent Intricacies: Engage not only with the puzzles but also with the silent intricacies woven into the physical challenges. Decrypt messages, decipher patterns, and embrace the essence of Defcon as you navigate the unseen and the tangible. Embark on the Engage Journey: ? Cube calls upon the curious and the bold. Embark on a journey where the puzzles transcend the digital divide, demanding both mental acuity and physical prowess.
H4QEG5LCMUQEAICEMVTGG33OEAZTEICSMVQWI6JAORXSAZLOM5QWOZJ7

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 14:00-14:59 PDT

Title: "BYOCTF" - Bring Your Own [Challenges||Capture] The Flag
When: Friday, Aug 9, 14:00 - 14:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

One of the best ways to learn something is to teach others about it. BYOCTF is a CTF framework (really a concept) that allows CTF players to contribute challenges for other players to solve and earn points as a reward. The purpose of the framework is to allow people to think about the learning experience of others. Everyone can learn how to become a CTF challenge developer.

SpeakerBio: Eli McRae, Penetration Tester

I'm a hacker person that sometimes does cool things. Hacker, husband, and father of 4 (2 human, 2 dogs). Veteran and occasional entrepreneur. I have worked in automation, security, development, infrastructure orchestration, training, network and software administration, and support. Full-stack IT FTW. Currently, I work as a penetration tester for a shipping and logistics firm. Previously, I worked as a trainer on behalf of the Arkansas Dept. of Education where taught both Cybersecurity and Computer Science concepts to public school teachers all across Arkansas (under previous governor, not the current one.). See more about that here.

Remember kids, hacking is more than the bad actions of bad actors.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 11:00-11:45 PDT

Title: (|(MaLDAPtive:¯_(LDAP)_/¯=ObFUsc8t10n) (De-Obfuscation &:=De*te)(!c=tion))
When: Sunday, Aug 11, 11:00 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

LDAP is no stranger to the security spotlight. While LDAP is a protocol (Lightweight Directory Access Protocol) and Active Directory is the most popular directory services system that supports a subset of LDAP, the terms “LDAP” and “AD” are tightly coupled when discussing the execution, detection and prevention of attacks targeting directory services data.

In the last decade the widespread offensive value of querying AD data via LDAP was cemented with the release of open-source tools such as BloodHound and PingCastle. However, proper visibility of LDAP queries mostly remains a privileged asset for those organizations with deep pockets, and the commercial security tools providing this visibility are often woefully fixated on simple signature-based detections.

MaLDAPtive is the 2,000-hour (and counting) quest of offensive and defensive LDAP exploration and tool-building. This research includes mind-bending depths of obfuscation across all elements of LDAP queries (many undocumented and most never seen in the wild), all baked into an obfuscation/de-obfuscation/detection framework built upon our ground-up custom LDAP search filter tokenizer and syntax tree parser.

Come witness the release of our MaLDAPtive research and open-source framework: transforming LDAP from “lightweight” to “heavyweight.”

- General LDAP information:
  - ♦ link
  - ♦ link
- LDAP-Related RFCs:
  - ♦ link
  - ♦ link
  - ♦ link
- Official Documentation for Active Directory LDAP Attributes: link
- Blogs Highlighting Offensive LDAP Usage:
  - ♦ link
  - ♦ link
  - ♦ link
  - ♦ link
- Open-Source Tooling Using LDAP:
  - ♦ link
  - ♦ link
  - ♦ link
  - ♦ link

Speakers: Daniel Bohannon,Sabajete Elezaj

SpeakerBio: Daniel Bohannon, Principal Threat Researcher, P0 Labs team at Permiso Security

Daniel Bohannon is a Principal Threat Researcher on Permiso Security's P0 Labs team with over 14 years of information security experience, including incident response consulting at MANDIANT, security research at FireEye and threat hunting at Microsoft.

He is the author of the Invoke-Obfuscation, Invoke-CradleCrafter and Invoke-DOSfuscation open-source obfuscation frameworks and co-author of Revoke-Obfuscation and Cloud Console Cartographer.

Mr. Bohannon received a Master of Science in Information Security from the Georgia Institute of Technology (2013) and a Bachelor of Science in Computer Science from The University of Georgia (2010).

SpeakerBio: Sabajete Elezaj, Senior Cyber Security Engineer at Solaris SE

Sabajete Elezaj is a Senior Cyber Security Engineer at Solaris SE with a background in cybersecurity extending over 6 years. Her expertise spans incident response, threat hunting and blue team operations. Her work focuses on enhancing cyber defense strategies.

Mrs. Elezaj holds a Master of Science in Information Security from the University of Tirana. She has also shared her expertise at cybersecurity conferences, including BSides Tirana.

Return to Index - Add to Google - ics Calendar file

Title: [CANCELED] AutoDriving CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05-B - Map

Description:

The AutoDriving CTF contest focuses on the emerging security challenges in autonomous driving systems. Various levels of self-driving functionalities, such as AI-powered perception, sensor fusion and route planning, are entering the product portfolio of automobile companies. From the security perspective, these AI-powered components not only contain common security problems such as memory safety bugs, but also introduce new threats such as physical adversarial attacks and sensor manipulations. Two popular examples of physical adversarial attacks are camouflage stickers that interfere with vehicle detection systems, and road graffitis that disturb lane keeping systems. The AI-powered navigation and control relies on the fusion of multiple sensor inputs, and many of the sensor inputs can be manipulated by malicious attackers. These manipulations combined with logical bugs in autonomous driving systems pose severe threats to road safety.

We design autonomous driving CTF (AutoDriving CTF) contests around the security challenges specific to these self-driving functions and components.

The goals of the AutoDriving CTF are the followings:

- Demonstrate security implications of autonomous driving system design decisions through hands-on challenges, increase the awareness of potential risks in security professionals, and encourage them to propose defense solutions and tools to detect such risks.
- Provide CTF challenges that allow players to learn attack and defense practices related to autonomous driving in a well-controlled, repeatable, and visible environment.
- Build a set of vulnerable autonomous driving components that can be used for security research and defense evaluation.

The contest is based on a Jeopardy style of CTF game with a set of independent challenges. A typical contest challenge includes a backend that runs autonomous driving components in simulated or real environments, and a frontend that interacts with the players. This year's contest will follow the style of last year and includes the following types of challenges:

- “attack”: such as constructing adversarial patches and spoofing fake sensor inputs,
- “forensics”: such as investigating a security incident related to autonomous driving,
- “detection”: such as detecting spoofed sensor inputs and fake obstacles,
- “crashme on road!”: such as creating dangerous traffic scenarios to expose logical errors in autonomous driving systems.
- “smart planner”: such as creating intelligent path planners for dangerous tasks that are difficult for human drivers

Most of these challenges will be developed using game-engine based autonomous driving simulators, such as CARLA and SVL. The following link contains some challenge videos, summaries from AutoDriving CTF at DEF CON 29 and DEF CON 30 https://drive.google.com/drive/folders/1JSVarIaQBmseLC9XqkfrxnRQto4WM225?usp=sharing https://www.youtube.com/channel/UCPPsKbVpxwk-464KIzr8xKw

What's new in 2024

This year, we will unlock new traffic conflict scenarios that are observed from real-world driving logs such as Jaywalk and double parked vehicles. New difficulty levels will be added to challenges in such scenarios by integrating real downstream AI modules such as object tracking from open-source autonomous driving software like Apollo, Autoware and OpenPilot.

In order to enable the audience to experience the challenges more directly, we plan to set up a vehicle wheel controller on site and provide a driving game this year. Audiences can drive themselves to compete with the self-driving vehicle in some of the challenges. Driving game demo: https://drive.google.com/drive/folders/1LIzJJ1I3Eqj_e0_ntX5eFu82U9ObiEYB?usp=sharing

For players

- What do players need to do to participate AutoDriving CTF? Most of the challenges do not require domain knowledge of autonomous driving software or adversarial machine learning, although knowledge of those helps. For example, the players can generate images the way they like (e.g., drawing, photoshopping) to fool the AI-components or write a short python script to control the vehicle. Some challenges, such as incident forensics likely would require players to learn domain knowledge such as sensor information format and how fusion works.
- What do we expect players to learn through the CTF event? Players can (1) gain a deep understanding of real-world autonomous driving systems' design, implementation, and their corresponding security properties and characteristics; and (2) learn the attack and defense practices related to autonomous driving in a well-controlled, repeatable, visible, and engaging environment.

Return to Index - Add to Google - ics Calendar file

Title: [CANCELED] AutoDriving CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05-B - Map

Description:

The AutoDriving CTF contest focuses on the emerging security challenges in autonomous driving systems. Various levels of self-driving functionalities, such as AI-powered perception, sensor fusion and route planning, are entering the product portfolio of automobile companies. From the security perspective, these AI-powered components not only contain common security problems such as memory safety bugs, but also introduce new threats such as physical adversarial attacks and sensor manipulations. Two popular examples of physical adversarial attacks are camouflage stickers that interfere with vehicle detection systems, and road graffitis that disturb lane keeping systems. The AI-powered navigation and control relies on the fusion of multiple sensor inputs, and many of the sensor inputs can be manipulated by malicious attackers. These manipulations combined with logical bugs in autonomous driving systems pose severe threats to road safety.

We design autonomous driving CTF (AutoDriving CTF) contests around the security challenges specific to these self-driving functions and components.

The goals of the AutoDriving CTF are the followings:

- Demonstrate security implications of autonomous driving system design decisions through hands-on challenges, increase the awareness of potential risks in security professionals, and encourage them to propose defense solutions and tools to detect such risks.
- Provide CTF challenges that allow players to learn attack and defense practices related to autonomous driving in a well-controlled, repeatable, and visible environment.
- Build a set of vulnerable autonomous driving components that can be used for security research and defense evaluation.

The contest is based on a Jeopardy style of CTF game with a set of independent challenges. A typical contest challenge includes a backend that runs autonomous driving components in simulated or real environments, and a frontend that interacts with the players. This year's contest will follow the style of last year and includes the following types of challenges:

- “attack”: such as constructing adversarial patches and spoofing fake sensor inputs,
- “forensics”: such as investigating a security incident related to autonomous driving,
- “detection”: such as detecting spoofed sensor inputs and fake obstacles,
- “crashme on road!”: such as creating dangerous traffic scenarios to expose logical errors in autonomous driving systems.
- “smart planner”: such as creating intelligent path planners for dangerous tasks that are difficult for human drivers

Most of these challenges will be developed using game-engine based autonomous driving simulators, such as CARLA and SVL. The following link contains some challenge videos, summaries from AutoDriving CTF at DEF CON 29 and DEF CON 30 https://drive.google.com/drive/folders/1JSVarIaQBmseLC9XqkfrxnRQto4WM225?usp=sharing https://www.youtube.com/channel/UCPPsKbVpxwk-464KIzr8xKw

What's new in 2024

This year, we will unlock new traffic conflict scenarios that are observed from real-world driving logs such as Jaywalk and double parked vehicles. New difficulty levels will be added to challenges in such scenarios by integrating real downstream AI modules such as object tracking from open-source autonomous driving software like Apollo, Autoware and OpenPilot.

In order to enable the audience to experience the challenges more directly, we plan to set up a vehicle wheel controller on site and provide a driving game this year. Audiences can drive themselves to compete with the self-driving vehicle in some of the challenges. Driving game demo: https://drive.google.com/drive/folders/1LIzJJ1I3Eqj_e0_ntX5eFu82U9ObiEYB?usp=sharing

For players

- What do players need to do to participate AutoDriving CTF? Most of the challenges do not require domain knowledge of autonomous driving software or adversarial machine learning, although knowledge of those helps. For example, the players can generate images the way they like (e.g., drawing, photoshopping) to fool the AI-components or write a short python script to control the vehicle. Some challenges, such as incident forensics likely would require players to learn domain knowledge such as sensor information format and how fusion works.
- What do we expect players to learn through the CTF event? Players can (1) gain a deep understanding of real-world autonomous driving systems' design, implementation, and their corresponding security properties and characteristics; and (2) learn the attack and defense practices related to autonomous driving in a well-controlled, repeatable, visible, and engaging environment.

Return to Index - Add to Google - ics Calendar file

Title: [CANCELED] AutoDriving CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: Virtual

Description:

The AutoDriving CTF contest focuses on the emerging security challenges in autonomous driving systems. Various levels of self-driving functionalities, such as AI-powered perception, sensor fusion and route planning, are entering the product portfolio of automobile companies. From the security perspective, these AI-powered components not only contain common security problems such as memory safety bugs, but also introduce new threats such as physical adversarial attacks and sensor manipulations. Two popular examples of physical adversarial attacks are camouflage stickers that interfere with vehicle detection systems, and road graffitis that disturb lane keeping systems. The AI-powered navigation and control relies on the fusion of multiple sensor inputs, and many of the sensor inputs can be manipulated by malicious attackers. These manipulations combined with logical bugs in autonomous driving systems pose severe threats to road safety.

We design autonomous driving CTF (AutoDriving CTF) contests around the security challenges specific to these self-driving functions and components.

The goals of the AutoDriving CTF are the followings:

- Demonstrate security implications of autonomous driving system design decisions through hands-on challenges, increase the awareness of potential risks in security professionals, and encourage them to propose defense solutions and tools to detect such risks.
- Provide CTF challenges that allow players to learn attack and defense practices related to autonomous driving in a well-controlled, repeatable, and visible environment.
- Build a set of vulnerable autonomous driving components that can be used for security research and defense evaluation.

The contest is based on a Jeopardy style of CTF game with a set of independent challenges. A typical contest challenge includes a backend that runs autonomous driving components in simulated or real environments, and a frontend that interacts with the players. This year's contest will follow the style of last year and includes the following types of challenges:

- “attack”: such as constructing adversarial patches and spoofing fake sensor inputs,
- “forensics”: such as investigating a security incident related to autonomous driving,
- “detection”: such as detecting spoofed sensor inputs and fake obstacles,
- “crashme on road!”: such as creating dangerous traffic scenarios to expose logical errors in autonomous driving systems.
- “smart planner”: such as creating intelligent path planners for dangerous tasks that are difficult for human drivers

Most of these challenges will be developed using game-engine based autonomous driving simulators, such as CARLA and SVL. The following link contains some challenge videos, summaries from AutoDriving CTF at DEF CON 29 and DEF CON 30 https://drive.google.com/drive/folders/1JSVarIaQBmseLC9XqkfrxnRQto4WM225?usp=sharing https://www.youtube.com/channel/UCPPsKbVpxwk-464KIzr8xKw

What's new in 2024

This year, we will unlock new traffic conflict scenarios that are observed from real-world driving logs such as Jaywalk and double parked vehicles. New difficulty levels will be added to challenges in such scenarios by integrating real downstream AI modules such as object tracking from open-source autonomous driving software like Apollo, Autoware and OpenPilot.

In order to enable the audience to experience the challenges more directly, we plan to set up a vehicle wheel controller on site and provide a driving game this year. Audiences can drive themselves to compete with the self-driving vehicle in some of the challenges. Driving game demo: https://drive.google.com/drive/folders/1LIzJJ1I3Eqj_e0_ntX5eFu82U9ObiEYB?usp=sharing

For players

- What do players need to do to participate AutoDriving CTF? Most of the challenges do not require domain knowledge of autonomous driving software or adversarial machine learning, although knowledge of those helps. For example, the players can generate images the way they like (e.g., drawing, photoshopping) to fool the AI-components or write a short python script to control the vehicle. Some challenges, such as incident forensics likely would require players to learn domain knowledge such as sensor information format and how fusion works.
- What do we expect players to learn through the CTF event? Players can (1) gain a deep understanding of real-world autonomous driving systems' design, implementation, and their corresponding security properties and characteristics; and (2) learn the attack and defense practices related to autonomous driving in a well-controlled, repeatable, visible, and engaging environment.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 16:40-17:10 PDT

Title: 0.0.0.0 Day: Exploiting Localhost APIs From The Browser
When: Saturday, Aug 10, 16:40 - 17:10 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Browser-based attacks are not new in the malicious landscape of attack patterns. Browsers remain a popular infiltration method for attackers.

While seemingly local, services running on localhost are accessible to the browser using a flaw we found, exposing the ports on the localhost network interface, and leaving the floodgates ajar to remote network attacks.

In this live demo and attack simulation we'll unveil a zero-day vulnerability (still under responsible disclosure) in Chrome and other browsers, and how we use the 0-day to attack developers behind firewalls. We will demonstrate remote code execution on a wildly popular open-source platform serving millions in the data engineering ecosystem, that seems to run on localhost.

In our talk, we will present novel attack techniques, targeting developers and employees within an organization, that are behind firewalls. This will be a first-ever deep dive into this newly discovered zero-day vulnerability.

Speakers:
Avi Lumelsky,Gal Elbaz

SpeakerBio:
Avi Lumelsky

Avi has a relentless curiosity about business, AI, security—and the places where all three connect. An experienced software engineer and architect, Avi's cybersecurity skills were first honed in elite Israeli intelligence units. His work focuses on privacy in the age of AI and big data.

SpeakerBio:
Gal Elbaz

Co-founder & CTO at Oligo Security with 10+ years of experience in vulnerability research and practical hacking. He previously worked as a Security Researcher at CheckPoint and served in the IDF Intelligence. In his free time, he enjoys playing CTFs.

Return to Index - Add to Google - ics Calendar file

ESV - Saturday - 10:00-17:59 PDT

Title: 101 Labs: Firmware and Software exploitation
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

This series of self-guided labs will introduce even the most novice hacker to the world of embedded device firmware and software exploitation. First-come first-served, don't miss a chance try out these labs and get started with embedded device hacking.

Return to Index - Add to Google - ics Calendar file

ESV - Friday - 10:00-17:59 PDT

Title: 101 Labs: Firmware and Software exploitation
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

This series of self-guided labs will introduce even the most novice hacker to the world of embedded device firmware and software exploitation. First-come first-served, don't miss a chance try out these labs and get started with embedded device hacking.

Return to Index - Add to Google - ics Calendar file

ESV - Sunday - 10:00-12:59 PDT

Title: 101 Labs: Firmware and Software exploitation
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

This series of self-guided labs will introduce even the most novice hacker to the world of embedded device firmware and software exploitation. First-come first-served, don't miss a chance try out these labs and get started with embedded device hacking.

Return to Index - Add to Google - ics Calendar file

ESV - Sunday - 10:00-12:59 PDT

Title: 101 Labs: Hardware Lab
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

If you've never popped open an embedded device and tried to get a simple shell, this is the lab for you. This is a first-come first-served workshop where you can walk through the step by step instructions to finding and connecting to a debug interface on an embedded device.

Return to Index - Add to Google - ics Calendar file

ESV - Friday - 10:00-17:59 PDT

Title: 101 Labs: Hardware Lab
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

If you've never popped open an embedded device and tried to get a simple shell, this is the lab for you. This is a first-come first-served workshop where you can walk through the step by step instructions to finding and connecting to a debug interface on an embedded device.

Return to Index - Add to Google - ics Calendar file

ESV - Saturday - 10:00-17:59 PDT

Title: 101 Labs: Hardware Lab
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

If you've never popped open an embedded device and tried to get a simple shell, this is the lab for you. This is a first-come first-served workshop where you can walk through the step by step instructions to finding and connecting to a debug interface on an embedded device.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 12:00-12:45 PDT

Title: 3D Printing My Way to Sanity: The Self-Funding Hobby That Changed Everything
When: Saturday, Aug 10, 12:00 - 12:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:
SpeakerBio: Steve Dossey
No BIO available

Return to Index - Add to Google - ics Calendar file

BHV - Sunday - 12:00-12:30 PDT

Title: 3DU: Homo (e)x Machina
When: Sunday, Aug 11, 12:00 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

The future of healthcare is precise, personalized, and involves point of care with a wide variety of applications. Each application has its own unique set of challenges that change based on risk and the stakeholders' perspective. Foreseeing these challenges, in 2021 FDA issued the discussion paper 3D Printing Medical Devices at the Point of Care to expound upon pertinent challenges and request stakeholder feedback. Within this paper, the concept of the 3D Printing medical device production system (MDPS) as a medical device was presented. In this session, we will investigate the concept of the MDPS from the perspective of different stakeholders, the necessity of AI to make this in-hospital MDPS POC solution a reality, and the unique relationship the MDM and HDO must have to support the MDPS.

SpeakerBio: Lacey Harbour

Lacey is an AI enabler for healthcare. Lacey has been published on standards and guidances around AI and 3D printing at the point of care and is a globally recognized speaker. She is a strategic committee member and leader within the AI-Global Health Initiative (AI-GHI).

Return to Index - Add to Google - ics Calendar file

TCV - Saturday - 15:00-16:59 PDT

Title: 4G Frenzy
When: Saturday, Aug 10, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

"4G Frenzy: Delving into Advanced Telecom Security" explores telecom network security with a focus on 4G. It covers the basics of 2G, 3G, and 4G, highlighting key differences and advancements. The workshop examines legacy telecom threats, vulnerabilities, and historical attacks, then delves into 4G's security improvements. Topics include protocols, RAN and core security, authentication, encryption, voice services, roaming, and Diameter protocol weaknesses. Includes hands-on demos of 4G weaknesses, prevention techniques, and open-source 4G network setup

SpeakerBio: Vinod Shrimali

Vinod is a telecom security expert with over 8.5 years of experience, specializing in 5G security, penetration testing, satellite and maritime security, and developing cost-effective security strategies. He is dedicated to securing data, networks, and systems to ensure safe communication, staying ahead of industry trends, delivering robust defense against cyber-attacks, and maintaining compliance with industry standards.

Return to Index - Add to Google - ics Calendar file

TCV - Friday - 11:00-13:59 PDT

Title: 5G Fortress
When: Friday, Aug 9, 11:00 - 13:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

The "5G Security Infrastructure" workshop at DEFCON begins with an overview of 5G infrastructure security. Module 1 covers 5G security architecture, RAN architecture, deployment models, critical components, and assessment methods. Module 2 examines new 5G protocols and their security impacts, including SBA, HTTP2, JSON API, N32 interface, PFCP, and SEPP. Module 3 explores network access security, SIM card security, 5G AKA, SUPI, and SUCI. Module 4 presents a 5G threat case study, with hands-on activities in UE & PT configuration, RAN security, and API testing

SpeakerBio: Akib Sayyed, Founder and Director at Matrix Shell Technologies

Akib, Founder and Director of Matrix Shell Technologies, has over 12 years of experience in Telecom Security. He has served diverse telecom operators across India, Africa, and the Middle East, specializing in signaling protocols and technologies like GSM, UMTS, LTE, 5G, and VoLTE. He has led numerous penetration testing projects, disclosed a GSM vulnerability in 2012, and worked with various open-source telecom platforms. Akib has also delivered training at Black Hat and DEFCON, contributing significantly to the cybersecurity community. His education includes a Bachelor's in Engineering (CSE) and certifications in ISO 17025:2017 and 5G.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 10:00-11:45 PDT

Title: 5Ghoul Framework - 5G NR Attacks & 5G OTA Fuzzing
When: Saturday, Aug 10, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W305 - Map

Description:

5Ghoul Fuzzer is an over-the-air security testing tool and fuzzing framework that leverages a rogue 5G NR base station to systematically create test cases targeting 5G-capable smartphones or Qualcomm USB-based modems. Moreover, such framework contains test case scripts to launch attacks exploiting 10 implementation-level vulnerabilities ranging from DoS to Downgrades that affect commercial 5G modems from major chipset vendors such as Qualcomm and MediaTek. The tool is released open sourced, but it is also continuously experimented with newer devices. For example, there are two more 5G implementation vulnerabilities that are under embargo and will be released by the end of this month in the open source repository and website maintained for the project.

Speakers: Matheus Eduardo Garbelini,Sudipta Chattopadhyay

SpeakerBio: Matheus Eduardo Garbelini, Research Fellow at Singapore University of Technology and Design (SUTD)

Matheus Eduardo Garbelini is a Research fellow at Singapore University of Technology and Design (SUTD) and a White Hat Wireless Hacker by hobby. Through his research in wireless fuzzing, he discovered implementation vulnerabilities in the chipset of countless Bluetooth, Wi-Fi, and 5G commercial IoT devices.

SpeakerBio: Sudipta Chattopadhyay, Associate Professor at Singapore University of Technology and Design (SUTD)

Sudipta Chattopadhyay is an Associate Professor at Singapore University of Technology and Design (SUTD) and hacks code during his spare time. His general research interests lie in the broad area of cyber security including but not limited to security for AI, Wireless Technologies, and Internet of Things (IoTs). Together with Matheus, he discovered SweynTooth, BrakTooth and 5Ghoul, families of Bluetooth and 5G NR vulnerabilities that affected billions of devices worldwide.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: 5N4CK3Y Contest
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-B - Map

Description:

AND!XOR creates electronic badges filled with hacker challenges. We love doing this, especially coming up with unique ways for hackers to earn them. Introducing the newest member of our hacker-fam: 5N4CK3Y (Snackey). 5N4CK3Y is a vending machine hardware hacking project from AND!XOR. We retrofitted it into an IoT CTF based badge dispensing machine, bling and all. Find a flag on our web hosted CTF platform, you get a 5N4CK3Y dispense code, punch it in, and a badge is vended to you! There are a variety of challenges to earn a badge as well others to continue working on the badge itself once obtained. These span from hardware hacking, reverse engineering, OSINT, network security, and cryptography to name a few. There's a little bit of everything, so it's a perfect way to learn something at one of the many DEF CON villages and talking with people you meet, then attempt one of the CTF challenges to dispense a badge. Hardware hacking is our passion and we want people to learn on badges, but more importantly that there's a lot to learn at DEF CON so our CTF will hopefully serve a desire to learn something new and meet new friends while trying to earn a badge and hack it further.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: 5N4CK3Y Contest
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-B - Map

Description:

AND!XOR creates electronic badges filled with hacker challenges. We love doing this, especially coming up with unique ways for hackers to earn them. Introducing the newest member of our hacker-fam: 5N4CK3Y (Snackey). 5N4CK3Y is a vending machine hardware hacking project from AND!XOR. We retrofitted it into an IoT CTF based badge dispensing machine, bling and all. Find a flag on our web hosted CTF platform, you get a 5N4CK3Y dispense code, punch it in, and a badge is vended to you! There are a variety of challenges to earn a badge as well others to continue working on the badge itself once obtained. These span from hardware hacking, reverse engineering, OSINT, network security, and cryptography to name a few. There's a little bit of everything, so it's a perfect way to learn something at one of the many DEF CON villages and talking with people you meet, then attempt one of the CTF challenges to dispense a badge. Hardware hacking is our passion and we want people to learn on badges, but more importantly that there's a lot to learn at DEF CON so our CTF will hopefully serve a desire to learn something new and meet new friends while trying to earn a badge and hack it further.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: 5N4CK3Y Contest
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-B - Map

Description:

AND!XOR creates electronic badges filled with hacker challenges. We love doing this, especially coming up with unique ways for hackers to earn them. Introducing the newest member of our hacker-fam: 5N4CK3Y (Snackey). 5N4CK3Y is a vending machine hardware hacking project from AND!XOR. We retrofitted it into an IoT CTF based badge dispensing machine, bling and all. Find a flag on our web hosted CTF platform, you get a 5N4CK3Y dispense code, punch it in, and a badge is vended to you! There are a variety of challenges to earn a badge as well others to continue working on the badge itself once obtained. These span from hardware hacking, reverse engineering, OSINT, network security, and cryptography to name a few. There's a little bit of everything, so it's a perfect way to learn something at one of the many DEF CON villages and talking with people you meet, then attempt one of the CTF challenges to dispense a badge. Hardware hacking is our passion and we want people to learn on badges, but more importantly that there's a lot to learn at DEF CON so our CTF will hopefully serve a desire to learn something new and meet new friends while trying to earn a badge and hack it further.

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 12:30-13:59 PDT

Title: A Bug Hunter's Guide to Account Takeover
When: Saturday, Aug 10, 12:30 - 13:59 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

This is a hands-on workshop with a lab that will help students and attendees learn some of the common and interesting ways to takeover accounts or escalate access while looking for vulnerabilities in a web app. These labs are all based on valid and have been awarded bounties by multiple large organizations such as Amazon, Zoom, PayPal, Yahoo, and more!

Pre-Prerequisites - Basic understanding of web application hacking - Knowledge of Web Proxies - Working laptop - Working WiFi (Will not be doable without access to a working WiFi) - Caido (BurpSuite or similar works too!)

SpeakerBio: Ben "NahamSec" Sadeghipour, Hacking Hub

Ben Sadeghipour, also known as NahamSec, is an ethical hacker, content creator, and keynote speaker. With a passion for cybersecurity that began in his teenage years, Ben's professional journey as a bug bounty hunter took off in 2014. He has played a role in helping organizations identify and remediate thousands of security vulnerabilities across a wide range of web and mobile applications in tech giants such as Amazon, Apple, Google, Airbnb, Snapchat, Zoom, and even the US Department of Defense. Ben helps others learn ethical hacking, bug bounty hunting, and reconnaissance techniques. He has also created training materials and content for conferences such as OWASP, DEFCON, and BSides.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 17:30-17:59 PDT

Title: A dive into world of Aircraft PKI
When: Saturday, Aug 10, 17:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

From protecting Aircraft Software Parts to authenticating aircraft to ground networks, aircraft use PKI in their day-to-day operations. In this talk we will cover the typical use cases, technologies, and regulations in play and touch upon the emerging threat of the Post-Quantum world and what it could mean for the protection of embedded software we find on aircraft.

SpeakerBio: Matt Gaffney, Principal Engineer, Aircraft Cyber Operations at United Airlines

Gaffers is a Principal Engineer for Aircraft Cyber Operations with United Airlines. Since joining their team in 2022 he has been heavily involved in Aircraft PKI projects serving as the SME on the requirements and regulations.

He fell into cybersecurity while serving in the British Army. Having had a previous life in software development, Gaffers found his superiors sending anything IT-related his way. When he later rejoined civilian life he spent a few years bouncing around different industries as a cybersecurity contractor before finding a passion in the niche of aviation cyber. In 2022 he moved across the pond with impeccable timing to land a role at a major US airline.

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 12:15-12:59 PDT

Title: A Hacker's guide to PQC
When: Friday, Aug 9, 12:15 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

This talk is aimed at non-experts and anyone who wants to stay ahead of the curve in a world where encryption rules are about to change dramatically. Whether you believe cryptographically relevant quantum computers are 10 or 100 years away, the first steps towards cryptographic agility that are being mandated within a couple of years. We'll explore the mind-bending math behind lattice-based and other exotic cryptosystems. Then, we'll get our hands dirty, dissecting real-world attacks launched against the finalists in the NIST PQC competition. Pwn the future of cryptography!

SpeakerBio: Konstantinos Karagiannis

Konstantinos is the Director of Quantum Computing Services at Protiviti. He helps companies get ready for quantum opportunities and threats. He has been involved in the quantum computing industry since 2012, and in InfoSec since the 90s. He is a frequent speaker at RSA, Black Hat, Defcon, and dozens of conferences worldwide. He hosts Protiviti's Post-Quantum World podcast and is our Venerable Village Elder here at Quantum Village.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 12:00-12:59 PDT

Title: A hole in one: pwning a cruise ship from a golf simulator and other tales of maritime IT-OT misconvergence
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

Andrew is formally a ships engineer and now spends much of his time pen testing ships. Along the way he's found the weirdest ways that IT/OT segregation has been broken, often through 3rd party technology suppliers. From VDRs to ICMS to safety management systems to fire control to azipods to... you name it he's broken it.

Cruising adds another layer of complexity, bringing together customer entertainment, restaurant and billing systems. The scope for segregation errors is multiplied.

The headline of this talk is tale about a misconfigured golf simulator onboard, that led to compromise of almost the entire vessel.

SpeakerBio: Andrew Tierney, Security Consultant at Pen Test Partners

Andrew leads PTP's hardware security team. He covers all systems that aren't general purpose computers e.g. ICS, IoT, phones, cars, ships, and planes. He has considerable experience of reverse engineering, researching, and finding vulnerabilities in these systems. He's a proficient electrical and electronics engineer, giving him great knowledge of underlying hardware and engineering.

He advises companies on building secure products. This ranges from the nitty-gritty of securing devices against physical attack, through to developing complete connected platforms that make use of defence-in-depth. He trains people on how to attack and defend hardware, with customers ranging from medical device manufacturers through to police forensics teams. Andrew has presented at DEF CON, BlackHat, hardwear.io, 44CON, multiple BSides events, and to private audiences such as the GSMA and NCSC.

Return to Index - Add to Google - ics Calendar file

AIxCC - Saturday - 15:45-16:30 PDT

Title: A Reverse Engineer's Guide to AI Interpretability
When: Saturday, Aug 10, 15:45 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

While the world buzzes about AI-augmented reverse engineering, what about turning the tables and reverse engineering AI itself? As artificial intelligence systems grow increasingly complex and pervasive, decoding their inner workings has become not just a fun challenge, but a critical necessity. This talk introduces the emerging field of mechanistic interpretability to the reverse engineering community, revealing how the frontier of AI research is reinventing wheels long familiar to RE experts. We'll explore how traditional reverse engineering techniques are finding new life in dissecting neural networks, and why the RE community's hard-earned wisdom is more relevant than ever in the age of AI.

SpeakerBio: Dr. Andrew Fasano, Cyber System Assessments at MIT Lincoln Laboratory

Dr. Andrew Fasano is a member of the technical staff in the Cyber System Assessment group at MIT Lincoln Laboratory. A former DEF CON CTF team captain, he holds a PhD from Northeastern University and is a maintainer of multiple open-source reverse engineering tools. Recently, Dr. Fasano has been applying his reverse engineering expertise to the emerging field of AI interpretability.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 15:00-15:45 PDT

Title: A Shadow Librarian in Broad Daylight: Fighting back against ever encroaching capitalism
When: Saturday, Aug 10, 15:00 - 15:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

The public library is under attack. Calls for book banning are at an all time high. Some states have passed laws that hold librarians legally accountable for offering "unacceptable" materials to minors. But before this fire started, another one was already burning. In an era of digital content, from eBooks to streaming movies, public libraries have been forced to accept draconian terms of service at the expense of their patrons and to the benefit of corporations. Grossly inflated eBook prices and licensing, unobtainable materials that went out of print due to artificial scarcity, exorbitant fees for access to academic research; these are just a few of the myriad of ways that libraries have been forced to bow before capitalism, all because of a desire to serve the public. But we can fight back...

And no one says we need to fight fairly.

I'd like to tell you some real life stories of a public librarian with a quasi-legal, dark grey skillset. And I'd love to share some ideas about what you can do to help others. If I can do this, you can. And anyone can be a shadow librarian.

1. Bodó, Balázs, Dániel Antal, and Zoltán Puha. "Can Scholarly Pirate Libraries Bridge the Knowledge Access Gap? An Empirical Study on the Structural Conditions of Book Piracy in Global and European Academia." Edited by Sergi Lozano. PLOS ONE 15, no. 12 (December 3, 2020): e0242509. link.
2. Böök, Mikael. "Herding the Wind," 2020. link.
3. Brown, Elizabeth Nolon. "You Can't Stop Pirate Libraries." Reason, 2022. link.
4. Complutense, Francisco Segado-Bo, Juan Martín-Quevedo, and Juan-José Prieto-Gutiérrez. "Jumping over the Paywall: Strategies and Motivations for Scholarly Piracy and Other Alternatives." Accessed January 4, 2024. link.
5. Gardner, Gabriel J, Stephen R McLaughlin, and Andrew D Asher. "Shadow Libraries and You: Sci-Hub Usage and the Future of ILL." ACRL 2017, Baltimore, Maryland, March 22 - 25, 2017. [Conference Paper], 2017. link.
6. Yesberg, Helen. "Libraries, Piracy and the Grey Area In-Between: Free Digital Media during the COVID-19 Pandemic." Reinvention: An International Journal of Undergraduate Research 15, no. 1 (April 29, 2022). link.

SpeakerBio: Daniel Messer

Dan is a systems librarian and SQL hacker living in Alvaton and Louisville, Kentucky. After almost 30 years of library work, he's cultivated a broad background in public library circulation methodology, library technology and automation, training and instruction, and library databases. A shadow librarian for ten years, he's provided cataloguing and scanning for various shadow libraries and online digital collections. And he's called upon his work in shadow libraries to help patrons as a traditional public librarian.

Beyond the library, he's an author, podcaster, musician, and coder.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 16:00-16:25 PDT

Title: A Short Introduction to 802.11ah Long Range WiFi HaLow with TaiXin TXW8301 devices
When: Friday, Aug 9, 16:00 - 16:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

This presentation is a practical introduction into 802.11ah HaLow WiFi. It starts with a brief description of the IEEE 802.11ah standard, history, and specification and includes a short survey of currently available 802.11ah chipsets and devices. One of these, the TaiXin TXW8301 chipset, is described in detail including hardware, firmware, configuration, and software tools. The radio waveform characteristics are presented as is information in using SDRs to capture and decode the WiFi frames. The presentation concludes with a brief description of the practical uses of 802.11ah devices.

Speakers: Ronald Broberg,Robert Van Etta

SpeakerBio: Ronald Broberg, Dark Wolf Solutions

Ronald Broberg is a cyber security engineer formerly with Lockheed Martin and currently with Dark Wolf Solutions where he hacks drones, clones, and cellular phones.

SpeakerBio: Robert Van Etta, Senior Penetration Tester at Dark Wolf Solutions

Robert Van Etta has 19 years of experience in hacking embedded systems and firmware analysis. He has previously worked in USAF Cyber Defense Operations and is now a Senior Penetration Tester at Dark Wolf Solutions.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 17:00-17:45 PDT

Title: A Treasure Trove of Failures: What History's Greatest Heist Can Teach Us About Defense In Depth
When: Saturday, Aug 10, 17:00 - 17:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

What's the real life equivalent of hacking a Gibson? Probably stealing hundreds of millions of dollars in diamonds, gold, and cash from one of the world's most formidable vaults. In 2003, a team of thieves did just that. Armed with hairspray, double sided tape, and nerves of steel, these thieves defeated layer after layer of security to pull off the haul of a lifetime.

However, as much as this is a story of skilled criminals, it is every bit as much a story of security failures and the parallels between protecting diamonds and data. In this presentation we'll dive deep into what went right, what went wrong, and how to properly apply defense in depth to make your security program look like a hundred million bucks.

1. Davis, J. (2009, March 12). The untold story of the World's biggest Diamond Heist. Wired. link
2. Selby, S. A., & Campbell, G. (2012). Flawless: Inside the largest diamond heist in history. Sterling.
3. Stegemeyer, P. (2021). Heist: An inside look at the world's 100 Greatest Heists, cons, and capers: From burglaries to bank jobs and everything in between. Whalen Book Works.

SpeakerBio: Pete Stegemeyer, Host at "I Can Steal That!" Podcast

Pete Stegemeyer is both a Senior Security Engineer and one of the world's leading heist experts. Pete has served as a consultant for Vice, National Geographic, and was a featured expert on the History Channel's series "History's Greatest Heists." He is the author of the best selling book Heist: An Inside Look at the World's 100 Greatest Heists, Cons and Capers and hosts of the popular podcast "I Can Steal That!"

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-15:59 PDT

Title: A Wall of Bribes
When: Saturday, Aug 10, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

This is a contest about bribery. Bribery is not only allowed, it is required as part of the contest, since it's the only way to move up the leaderboard. Judges will evaluate the value of any given bribe (for example, an unusual sticker, etc.), and award points accordingly. Boring bribes will be rejected (i.e. cash). Players can expect to learn how to make a persuasive argument, and the nature of value in an (often) pay-to-win world that we live in.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: A Wall of Bribes
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

This is a contest about bribery. Bribery is not only allowed, it is required as part of the contest, since it's the only way to move up the leaderboard. Judges will evaluate the value of any given bribe (for example, an unusual sticker, etc.), and award points accordingly. Boring bribes will be rejected (i.e. cash). Players can expect to learn how to make a persuasive argument, and the nature of value in an (often) pay-to-win world that we live in.

Return to Index - Add to Google - ics Calendar file

CPV - Saturday - 16:00-16:30 PDT

Title: A Whirlwind Tour of the FBI's Secret Encrypted Chat App
When: Saturday, Aug 10, 16:00 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

The FBI ran an encrypted app called Anom, intercepting all of its messages. The operation ended in the arrest of hundreds of criminals. But what happens now? Are apps that we all use, like Signal, under threat too? This talk will give a blistering dive into what the app was, how it worked, and what it means for all of our privacy now.

SpeakerBio: Joseph Cox, Co-Founder at 404 Media

Joseph Cox is an investigative journalist and author of DARK WIRE, the inside story of how the FBI secretly ran its own encrypted phone company called Anom to wiretap the world. He produced a series of exclusive articles on Anom for VICE's Motherboard, and is now a co-founder of 404 Media.

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 12:15-13:45 PDT

Title: A Zero to Hero Crash Course to Server-Side Request Forgery (SSRF)
When: Friday, Aug 9, 12:15 - 13:45 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

Server-Side Request Forgery is now one of the most widely recognized and significant vulnerabilities that bug hunters should have in their arsenal. This interactive workshop covers basic exploitation of SSRF, as well as tackling more intricate vulnerabilities that involve chaining multiple exploits, a thorough comprehension of the target's infrastructure, and other advanced techniques.

Pre-Prerequisites

- Basic understanding of web application hacking
- Knowledge of Web Proxies
- Working laptop
- Working WiFi (Will not be doable without access to a working WiFi)
- Caido (BurpSuite or similar works too!)

SpeakerBio: Ben "NahamSec" Sadeghipour, Hacking Hub

Ben Sadeghipour, also known as NahamSec, is an ethical hacker, content creator, and keynote speaker. With a passion for cybersecurity that began in his teenage years, Ben's professional journey as a bug bounty hunter took off in 2014. He has played a role in helping organizations identify and remediate thousands of security vulnerabilities across a wide range of web and mobile applications in tech giants such as Amazon, Apple, Google, Airbnb, Snapchat, Zoom, and even the US Department of Defense. Ben helps others learn ethical hacking, bug bounty hunting, and reconnaissance techniques. He has also created training materials and content for conferences such as OWASP, DEFCON, and BSides.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: A-ISAC Aviation Cybersecurity Challenge
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

A variety of aviation infrastructure has been compromised by hackers. Immerse yourself into challenges where you are tasked as an aviation cyber defense participant to identify attacks/attackers, stop attacks, and restore normal operations. As a participant your first step is to register ahead and read the rules at: https://aisac.cyberskyline.com/events/aisac-defcon and bring your own laptop to the venue. You can participate in the virtual challenges from Friday, but the more critical in-person challenges are only available at certain times during Village open hours!

SpeakerBio: A-ISAC and Embry-Riddle Aeronautical University - Prescott
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: A-ISAC Aviation Cybersecurity Challenge
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

A variety of aviation infrastructure has been compromised by hackers. Immerse yourself into challenges where you are tasked as an aviation cyber defense participant to identify attacks/attackers, stop attacks, and restore normal operations. As a participant your first step is to register ahead and read the rules at: https://aisac.cyberskyline.com/events/aisac-defcon and bring your own laptop to the venue. You can participate in the virtual challenges from Friday, but the more critical in-person challenges are only available at certain times during Village open hours!

SpeakerBio: A-ISAC and Embry-Riddle Aeronautical University - Prescott
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: A-ISAC Aviation Cybersecurity Challenge
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

A variety of aviation infrastructure has been compromised by hackers. Immerse yourself into challenges where you are tasked as an aviation cyber defense participant to identify attacks/attackers, stop attacks, and restore normal operations. As a participant your first step is to register ahead and read the rules at: https://aisac.cyberskyline.com/events/aisac-defcon and bring your own laptop to the venue. You can participate in the virtual challenges from Friday, but the more critical in-person challenges are only available at certain times during Village open hours!

SpeakerBio: A-ISAC and Embry-Riddle Aeronautical University - Prescott
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 12:00-12:59 PDT

Title: Abusando de Bitlocker para secuestrar información corporativa | Desde la intrusión hasta el descifrado (i)
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Durante abril de 2024 el equipo GERT de Kaspersky detectó un nuevo grupo de ransomware aprovechando las funcionalidades de Microsoft para cifrar sistemas en infraestructuras comprometidas, usando scripts para disminuir defensas, deshabilitar parámetros críticos de sistemas Microsoft y finalmente usar el servicio Bitlocker de Microsoft, creando contraseñas individuales de cifrado por cada sistema, eliminando los rastros locales y enviando los datos mediante comunicaciones de comando y control para garantizar el descifrado y recibir el pago del rescate. Aunque el ataque fue dirigido a organizaciones en LATAM, fue identificado también en Jordania e Indonesia. Durante esta charla presentaremos los principales retos de recolectar evidencia en sistemas donde los discos fueron completamente cifrados y las propuestas de descifrado habilitadas una vez se obtuvo la muestra del malware construida de forma dirigida para las organizaciones afectadas. Se presentarán los mecanismos de descifrado disponibles frente a esta y otras amenazas similares y las técnicas usadas por los adversarios para comprometer las infraestructuras.

SpeakerBio: Eduardo Chavarro Ovalle, Digital Forensic and Incident Response Group Manager Americas

MSc Eduardo Chavarro Ovalle, DFIR Group Manager para Kaspersky GERT en América, especialista en respuesta a Incidentes, CSIRT Leader, MSc en seguridad informática, Ingeniero en Telecomunicaciones con conocimiento en Gerencia Estratégica de las Telecomunicaciones, con más de 20 años de experiencia en Análisis Digital Forense, Respuesta a Incidentes, eDiscovery, Threat Hunting, entre otros. GCIH | GRID | GCFA | CISM | CHFI | C)PTE | SFCP | ITIL

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 12:00-12:50 PDT

Title: Abusing DevOps to Pivot Between Cloud and On-Prem
When: Friday, Aug 9, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

As more scrutiny is placed on the endpoint, threat actors are turning to DevOps and CI/CD platforms for initial access, escalation, and lateral movement. This workshop will showcase how these platforms can be used to pivot from on-prem to cloud, from cloud to on-prem, and how to push malicious code through pipelines to obtain additional access or establish persistence.

Attendees will get hands-on and perform field-tested, OPSEC-conscious techniques against full CI/CD pipelines. Come add TTPs to your toolkit and see why DevOps is the target-rich environment modern adversaries are looking to exploit.

Speakers: Colbert Zhu,Tom Porter

SpeakerBio: Colbert Zhu
No BIO available
SpeakerBio: Tom Porter
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Abusing legacy railroad signaling systems
When: Sunday, Aug 11, 14:00 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

In this study, we delve into the darker aspects of railway technology, revealing how easily accessible domestic hardware tools can compromise the seemingly infallible robustness of signaling systems. We demonstrate how these accessible technologies can be utilized to devise strategies that potentially threaten train circulation in Spain. Our research presents a critical analysis of the vulnerabilities present in the railway signaling systems, highlighting the ease with which these systems can be tampered with, using tools that are readily available to the general public. Through a combination of theoretical insights and practical demonstrations, we offer a comprehensive overview of the risks associated with such vulnerabilities.

Our findings aim to raise awareness among stakeholders in the railway industry, prompting a reevaluation of current security measures and encouraging the adoption of more stringent protections against such threats. This paper contributes to the ongoing discussion in the cybersecurity community, offering valuable insights into the potential risks facing modern transportation infrastructures and suggesting avenues for future research and development in railway system security.

We consider this work to be innovative on a type of system that has been present for over half a century in railway infrastructures. Therefore, the references provided are primarily about the operation of the systems and relevant news concerning them.

1. link
2. link
3. link
4. link
5. link
6. link
7. link
8. link
9. link
10. link
11. link
12. link
13. link
14. link

Speakers: David Meléndez,Gabriela (Gabs) Garcia

SpeakerBio: David Meléndez, R&D Enginner and Red Team Member, Innotec Security at Accenture

David Melendez is an R&D Enginner and Red Team member at Innotec Security Part of Accenture, with over twelve years of experience in cybersecurity and hardware hacking. He has a proven track record of presenting his groundbreaking investigations at prestigious conferences around the world, including DEF CON, BLACKHAT, and ROOTEDCON.

David is also a drone creator and author of the book "Hacking with Drones," which showcases his innovative use of drones in cybersecurity research. With his passion for pushing the boundaries of technology, David is constantly seeking new ways to improve the security and functionality of embedded systems.

SpeakerBio: Gabriela (Gabs) Garcia

Gabriela (Gabs) García is a university professor and mentor, Secure Software Developer and coding and cybersecurity instructor for organizations such as LinkedIn, Cyber Hunter Academy and Kschool. She teaches, whether that's in a lecture hall or over the internet, about software development, with a keen eye for secure practices. She is a speakers in several hacking CONs like DEF CON USA, ROOTEDCON etc.

Gabriela is also an active member in hacker communities such as HackMadrid%27 and Hack%27, both at home in Spain and across the world. And as an independent professional, she gets to work with a wide variety of clients, crafting custom cybersecurity solutions to fit their specific needs.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 15:00-15:45 PDT

Title: Abusing Windows Hello Without a Severed Hand
When: Friday, Aug 9, 15:00 - 15:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

Windows Hello is touted by Microsoft as the modern de facto authentication scheme on Windows platforms, supporting authentication and encryption backed by biometrics. In a world that is quickly accelerating towards a passwordless existence, what new threats do we face in this complex landscape? We will take a deep dive into the inner working of Windows Hello. Via the release of a new tool, it will be demonstrated how an attacker on a fully compromised Windows host can leverage secrets backed by Windows Hello biometrics without needing the biometric data that protects them. We will also show how the hardware protections of Windows Hello and its accompanying Primary Refresh Tokens can be defeated, making it possible to use Windows Hello for identity persistency and PRT stealing, in some cases even without Administrator access on the host.

- link
- link
- link
- link
- link

Speakers: Ceri Coburn,Dirk-jan Mollema

SpeakerBio: Ceri Coburn, Red Team Operator and Offensive Security Dev at Pen Test Partners

After a 20 year career within the software development space, Ceri was looking for a new challenge and moved into pen testing back in 2019. During that time he has created and contributed to several open source offensive tools such as Rubeus, BOFNET and SweetPotato and on the odd occasion contributed to projects on the defensive side too. After speaking at DEF CON 31 for the first-time last year, he is now back for more. He currently works as a red team operator and offensive security dev at Pen Test Partners.

SpeakerBio: Dirk-jan Mollema, Security Researcher at Outsider Security

Dirk-jan Mollema is a hacker and researcher of Active Directory and Microsoft Entra (Azure AD) security. In 2022 he started his own company, Outsider Security, where he performs penetration tests and reviews of enterprise networks and cloud environments. He blogs at dirkjanm.io, where he publishes his research, and shares updates on the many open source security tools he has written over the years. He presented previously at TROOPERS, DEF CON, Black Hat and BlueHat and has been awarded as one of Microsoft's Most Valuable Researchers multiple times.

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 16:00-16:30 PDT

Title: Access Control done right the first time
When: Friday, Aug 9, 16:00 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Are you looking to install or upgrade a physical access control system? Having installed, repaired and upgraded dozens of large and small access control system installations, I have found that many vendors install a minimum viable product that can leave your new system unreliable and trivial to bypass.

This session will give you the tools and knowledge you need to work with your installer to implement your system using best practices in the following areas:

- Wiring, supervision, encryption and tamper-resistance
- Choosing clone-resistant badges and securely programming badge readers
- Securing controller equipment and managing issued badges
- Maintaining the system for maximum security and uptime

SpeakerBio: Tim Clevenger, Cybersecurity Network Engineer at SailPoint

As a low voltage hardware junkie, Tim has had the opportunity to design, expand, upgrade and repair numerous physical access control, alarm and video systems, including a stint at a security vendor where he was certified in Lenel access and video. Tim works today at SailPoint as a Cybersecurity Network Engineer.

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 15:30-15:59 PDT

Title: Access Control Done Right the First Time
When: Saturday, Aug 10, 15:30 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Are you looking to install or upgrade a physical access control system? Having installed, repaired and upgraded dozens of large and small access control system installations, I have found that many vendors install a minimum viable product that can leave your new system unreliable and trivial to bypass.

This session will give you the tools and knowledge you need to work with your installer to implement your system using best practices in the following areas:

- Wiring, supervision, encryption and tamper-resistance
- Choosing clone-resistant badges and securely programming badge readers
- Securing controller equipment and managing issued badges
- Maintaining the system for maximum security and uptime

SpeakerBio: Tim Clevenger, Cybersecurity Network Engineer at SailPoint

As a low voltage hardware junkie, Tim has had the opportunity to design, expand, upgrade and repair numerous physical access control, alarm and video systems, including a stint at a security vendor where he was certified in Lenel access and video. Tim works today at SailPoint as a Cybersecurity Network Engineer.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 14:30-15:15 PDT

Title: ACE up the Sleeve: From getting JTAG on the iPhone 15 to hacking into Apple's new USB-C Controller
When: Saturday, Aug 10, 14:30 - 15:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

With the iPhone 15 & iPhone 15 Pro Apple switched their iPhone to USB-C - and introduced a new proprietary USB-C controller: The ACE3.

But the ACE3 does more than just handle USB power delivery: It's a full microcontroller running a full USB stack connected to some of the internal busses of the device, and we even managed to access JTAG on the iPhone 15 through it. It also provides access to UART, the internal SPMI bus, etc. Previous variants of the ACE, namely the ACE2 found in MacBooks, could easily be dumped and analyzed using SWD - and even be persistently backdoored through a software vulnerability we found.

On the ACE3 however, Apple upped their game: Firmware updates are personalized, debug interfaces seem to be disabled, and the external flash is validated and does not contain all the firmware. However using a combination of reverse-engineering, RF side-channel analysis and electro-magnetic fault-injection it was possible to gain code-execution on the ACE3 - allowing dumping of the ROM, and analysis of the functionality.

This talk will show how to use a combination of hardware, firmware, reverse-engineering, side-channel analysis and fault-injection to gain code-execution on a completely custom chip, enabling further security research on an under-explored but security relevant part of Apple devices.

- AsahiLinux USB-PD Documentaiton - link
- AsahiLinux macvdmtool - link
- ACE Controller Secrets (for ACE/ACE2) - link
- Marc Zyngier's Central Scrutinizer - link

SpeakerBio: Thomas "stacksmashing" Roth

Thomas Roth aka stacksmashing is a security researcher mostly focused on hardware and firmware. His work includes hardware attacks on processors, microcontrollers and cryptocurrency wallets, building cheap JTAG tooling for the iPhone, and attacking a wide variety of embedded devices. He also runs a YouTube channel called stacksmashing about security, reverse engineering and hardware hacking.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 15:00-16:59 PDT

Title: Activity: API Security 101: Testing and Trivia by Akto.io
When: Saturday, Aug 10, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 3 - Map

Description:

In this activity, participants will see an API Security presentation with examples and engage in a trivia game centered around the topic.

Learn about the wide range of API vulnerabilities with real-world examples of data breaches and what it means to secure APIs through tests. And then it's trivia time!

Participants will have to answer 10-15 questions on API Security based on their learnings. You will get swags for each answer you get right!

Speakers: Ankush Jain,Ankita Gupta

SpeakerBio: Ankush Jain, Co-founder & CTO at Akto

Ankush is the co-founder & CTO at Akto (https://www.akto.io). Prior to starting Akto he worked at CleverTap as VP of Engineering. He has also worked for 5 years as a Quant at Morgan Stanley. He has acquired US patents at Microsoft at CleverTap.

SpeakerBio: Ankita Gupta
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 11:00-12:59 PDT

Title: Activity: API Security 101: Testing and Trivia by Akto.io
When: Saturday, Aug 10, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 2 - Map

Description:

In this activity, participants will see an API Security presentation with examples and engage in a trivia game centered around the topic.

Learn about the wide range of API vulnerabilities with real-world examples of data breaches and what it means to secure APIs through tests. And then it's trivia time!

Participants will have to answer 10-15 questions on API Security based on their learnings. You will get swags for each answer you get right!

Speakers: Ankush Jain,Ankita Gupta

SpeakerBio: Ankush Jain, Co-founder & CTO at Akto

Ankush is the co-founder & CTO at Akto (https://www.akto.io). Prior to starting Akto he worked at CleverTap as VP of Engineering. He has also worked for 5 years as a Quant at Morgan Stanley. He has acquired US patents at Microsoft at CleverTap.

SpeakerBio: Ankita Gupta
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Friday - 13:00-14:59 PDT

Title: Activity: Capture the Container by Chainguard
When: Friday, Aug 9, 13:00 - 14:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 1 - Map

Description:

Join us for an exhilarating container security CTF where you can go head-to-head with your peers. In this session, we will explore the world of container security, including image analysis, enumeration, and the most up-to-date container escape techniques. Put your skills to the test and compete for the top spot! Participants will gain valuable knowledge in container security and have the chance to win some exciting prizes. Don't miss out on this thrilling opportunity to showcase your expertise!

SpeakerBio: Jonathan Leitschuh
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 11:00-12:59 PDT

Title: Activity: Capture the Container by Chainguard
When: Saturday, Aug 10, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 3 - Map

Description:

Join us for an exhilarating container security CTF where you can go head-to-head with your peers. In this session, we will explore the world of container security, including image analysis, enumeration, and the most up-to-date container escape techniques. Put your skills to the test and compete for the top spot! Participants will gain valuable knowledge in container security and have the chance to win some exciting prizes. Don't miss out on this thrilling opportunity to showcase your expertise!

SpeakerBio: Jonathan Leitschuh
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 11:00-12:59 PDT

Title: Activity: Hacking Developers' Trust – Faking GitHub Contribution by Checkmarx
When: Sunday, Aug 11, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 1 - Map

Description:

Join us for a revealing exploration of open-source trust and its vulnerabilities. In this captivating activity, we will delve into the fascinating world of developer credibility and the unsettling phenomenon of faking GitHub contributions. With open source becoming an integral part of software development, we find ourselves relying on strangers to provide us with code. Trust is often based on factors like the number of stars on a package or the credibility of the package's maintainer on GitHub. However, what if I told you that all of this could be convincingly spoofed?

Speakers:Tal Folkman,Ori Ron,Mário Leitão-Teixeira

SpeakerBio: Tal Folkman

Tal brings over 7 years of experience to her role as a supply chain security research team lead within Checkmarx Supply Chain Security group. She is in charge of detecting tracking and stopping Opensource attacks.

SpeakerBio: Ori Ron

Ori Ron, an experienced Application Security Researcher at Checkmarx, joined the company in 2016. With over eight years of expertise in the field, Ori specializes in identifying and mitigating security vulnerabilities in software systems. His research spans the application security aspects of many programming languages, technologies, and environments.

SpeakerBio: Mário Leitão-Teixeira

"Vulnerability" is part of my daily vocabulary at Checkmarx, and I never get sick of it. I dub myself a 'self-certified idiot' because I love learning and hatching ideas. So much, that I've made brainstorming a hobby and kickstarted a team initiative to keep us on the pulse of InfoSec. As a result, we have learned about CVSSv4 before it was cool.

Well, CVSSv4 isn't cool yet since it's yet to be fully adopted, but in the meantime, I've researched and come up with this talk. I wasn't given the opportunity to win a 'Best Speaker' award yet. However, I published a few blog posts for Checkmarx and am brewing many other initiatives. I'm also currently studying to pass the CEH certification. Contributing to the AppSec Village at RSAC in San Francisco last year. Check.

Beyond the keyboard, you catch me reading, writing, or practicing martial arts. As in cybersecurity, I seek constant learning.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 15:00-16:59 PDT

Title: Activity: Hacking Developers' Trust – Faking GitHub Contribution by Checkmarx
When: Friday, Aug 9, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 3 - Map

Description:

Join us for a revealing exploration of open-source trust and its vulnerabilities. In this captivating activity, we will delve into the fascinating world of developer credibility and the unsettling phenomenon of faking GitHub contributions. With open source becoming an integral part of software development, we find ourselves relying on strangers to provide us with code. Trust is often based on factors like the number of stars on a package or the credibility of the package's maintainer on GitHub. However, what if I told you that all of this could be convincingly spoofed?

Speakers:Tal Folkman,Ori Ron,Mário Leitão-Teixeira

SpeakerBio: Tal Folkman

Tal brings over 7 years of experience to her role as a supply chain security research team lead within Checkmarx Supply Chain Security group. She is in charge of detecting tracking and stopping Opensource attacks.

SpeakerBio: Ori Ron

Ori Ron, an experienced Application Security Researcher at Checkmarx, joined the company in 2016. With over eight years of expertise in the field, Ori specializes in identifying and mitigating security vulnerabilities in software systems. His research spans the application security aspects of many programming languages, technologies, and environments.

SpeakerBio: Mário Leitão-Teixeira

"Vulnerability" is part of my daily vocabulary at Checkmarx, and I never get sick of it. I dub myself a 'self-certified idiot' because I love learning and hatching ideas. So much, that I've made brainstorming a hobby and kickstarted a team initiative to keep us on the pulse of InfoSec. As a result, we have learned about CVSSv4 before it was cool.

Well, CVSSv4 isn't cool yet since it's yet to be fully adopted, but in the meantime, I've researched and come up with this talk. I wasn't given the opportunity to win a 'Best Speaker' award yet. However, I published a few blog posts for Checkmarx and am brewing many other initiatives. I'm also currently studying to pass the CEH certification. Contributing to the AppSec Village at RSAC in San Francisco last year. Check.

Beyond the keyboard, you catch me reading, writing, or practicing martial arts. As in cybersecurity, I seek constant learning.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 11:00-12:59 PDT

Title: Activity: Spot the Reachable by Backslash
When: Friday, Aug 9, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 3 - Map

Description:

Find the reachable one! You've got 18x18 inch game board, 5 cards, 5 code weaknesses, and a 5-minute sand timer, ready, set, go! You'll have 5 minutes to place the cards in the correct order and find the true positive(s). The winner? Whoever finds the solution in the shortest amount of time!

Speakers: Czesia Glik,Yossi Pik

SpeakerBio: Czesia Glik
No BIO available
SpeakerBio: Yossi Pik, CTO & Co-Founder at Backslash Security
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 13:00-14:59 PDT

Title: Activity: Spot the Reachable by Backslash
When: Saturday, Aug 10, 13:00 - 14:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 1 - Map

Description:

Find the reachable one! You've got 18x18 inch game board, 5 cards, 5 code weaknesses, and a 5-minute sand timer, ready, set, go! You'll have 5 minutes to place the cards in the correct order and find the true positive(s). The winner? Whoever finds the solution in the shortest amount of time!

Speakers: Czesia Glik,Yossi Pik

SpeakerBio: Czesia Glik
No BIO available
SpeakerBio: Yossi Pik, CTO & Co-Founder at Backslash Security
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 15:00-16:59 PDT

Title: Activity: Spot the Reachable by Backslash
When: Saturday, Aug 10, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 1 - Map

Description:

Find the reachable one! You've got 18x18 inch game board, 5 cards, 5 code weaknesses, and a 5-minute sand timer, ready, set, go! You'll have 5 minutes to place the cards in the correct order and find the true positive(s). The winner? Whoever finds the solution in the shortest amount of time!

Speakers: Czesia Glik,Yossi Pik

SpeakerBio: Czesia Glik
No BIO available
SpeakerBio: Yossi Pik, CTO & Co-Founder at Backslash Security
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 13:00-14:59 PDT

Title: Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian
When: Saturday, Aug 10, 13:00 - 14:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 3 - Map

Description:

Before you can deal with secrets sprawl, you first need to understand how deep the issue of plaintext secrets can be. Improperly stored and shared secrets are a problem beyond just the top layer of code you put in production. It affects feature branches, old commits, logs, and communication and collaboration tools.

In this exercise, you will be challenged to find all the secrets and then use a special tool to quickly validate the secrets and your work. Walk away from this exercise ready to apply the lessons learned to make your organization safer in no time.

SpeakerBio: mcdwayne

Dwayne has been working as a Developer Relations professional since 2015 and has been involved in tech communities since 2005. He loves sharing his knowledge, and he has done so by giving talks at over a hundred events worldwide. Dwayne currently lives in Chicago. Outside of tech, he loves karaoke, live music, and performing improv.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 11:00-12:59 PDT

Title: Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian
When: Friday, Aug 9, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 2 - Map

Description:

Before you can deal with secrets sprawl, you first need to understand how deep the issue of plaintext secrets can be. Improperly stored and shared secrets are a problem beyond just the top layer of code you put in production. It affects feature branches, old commits, logs, and communication and collaboration tools.

In this exercise, you will be challenged to find all the secrets and then use a special tool to quickly validate the secrets and your work. Walk away from this exercise ready to apply the lessons learned to make your organization safer in no time.

SpeakerBio: mcdwayne

Dwayne has been working as a Developer Relations professional since 2015 and has been involved in tech communities since 2005. He loves sharing his knowledge, and he has done so by giving talks at over a hundred events worldwide. Dwayne currently lives in Chicago. Outside of tech, he loves karaoke, live music, and performing improv.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 15:00-16:59 PDT

Title: Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian
When: Friday, Aug 9, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 2 - Map

Description:

Before you can deal with secrets sprawl, you first need to understand how deep the issue of plaintext secrets can be. Improperly stored and shared secrets are a problem beyond just the top layer of code you put in production. It affects feature branches, old commits, logs, and communication and collaboration tools.

In this exercise, you will be challenged to find all the secrets and then use a special tool to quickly validate the secrets and your work. Walk away from this exercise ready to apply the lessons learned to make your organization safer in no time.

SpeakerBio: mcdwayne

Dwayne has been working as a Developer Relations professional since 2015 and has been involved in tech communities since 2005. He loves sharing his knowledge, and he has done so by giving talks at over a hundred events worldwide. Dwayne currently lives in Chicago. Outside of tech, he loves karaoke, live music, and performing improv.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 13:00-14:59 PDT

Title: Activity: Test Your AppSec Knowledge by Deepfactor
When: Friday, Aug 9, 13:00 - 14:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 3 - Map

Description:

It's in the Cards! Pick 5 cards with random levels of difficulty. Answer questions ranging from true/false to multiple choice to spot the vulnerable code. Test your knowledge on risky deployment scenarios, rack up the points, and get to the top of the leaderboard to win!

SpeakerBio: Mike Larkin
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 11:00-12:59 PDT

Title: Activity: Threat modelling fun session with OWASP Cornucopia
When: Sunday, Aug 11, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 3 - Map

Description:

Join us into this collaborative game of OWASP Cornucopia! Over the course of two hours we will create a Threat Model of an example target infrastructure using the OWASP Cornucopia game! Winner keeps the deck!

SpeakerBio: Konstantinos Papapanagiotou

Konstantinos is the Advisory Services Director at Census Labs S.A. Prior to that, he worked for OTE S.A. (member of Deutsche Telekom Group) where he was responsible for the cyber security solutions offered to corporate customers. In the past he has led cyber security consulting teams in other private sector organizations. He has more than 20 years of experience in the field of cyber security both as a corporate consultant and as a researcher. During that time, he participated in numerous cyber security projects in public and private sector organizations, in Greece, Europe, and the Middle East. He has been an OWASP volunteer since 2004, leading the Greek chapter and contributing to several projects. He holds a PhD and BSc from the Department of Informatics and Telecommunications at the University of Athens, Greece, as well as a MSc in Information Security with distinction from Royal Holloway, University of London. For more than 10 years he served as an Adjunct Lecturer at the Hellenic American University, as well as the University of Athens and University of Piraeus, teaching Information Security to postgraduate and undergraduate students.

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 11:00-12:59 PDT

Title: Activity: Threat modelling fun session with OWASP Cornucopia
When: Sunday, Aug 11, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 2 - Map

Description:

Join us into this collaborative game of OWASP Cornucopia! Over the course of two hours we will create a Threat Model of an example target infrastructure using the OWASP Cornucopia game! Winner keeps the deck!

SpeakerBio: Andra

Andra is a Principal Application Security Specialist at Sage, with over seven years of experience in the field of application security. She is responsible for implementing DevSecOps practices, conducting security assessments, and developing secure coding guidelines for software engineering and AI/ML teams. She holds multiple certifications, including AWS Certified Cloud Practitioner and Attacking and Securing APIs. She has a strong background in software development and project management, as well as a master's degree in information and computer sciences. She has been co-leading the OWASP London Chapter since 2019, where she organises and delivers events and workshops on various security topics. She is passionate about educating and empowering developers and stakeholders to build and deliver secure software and best practices in a fast-paced, results-driven environment.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 11:00-12:59 PDT

Title: Activity: Vulnerability Hunt - The Snippets Edition
When: Saturday, Aug 10, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 1 - Map

Description:

Put your skills to the test in this challenge and try to find all the vulnerabilities in the code. We have a wide range of challenges, from easy to advanced in various languages. Can you find them all?

SpeakerBio: Mário Leitão-Teixeira

"Vulnerability" is part of my daily vocabulary at Checkmarx, and I never get sick of it. I dub myself a 'self-certified idiot' because I love learning and hatching ideas. So much, that I've made brainstorming a hobby and kickstarted a team initiative to keep us on the pulse of InfoSec. As a result, we have learned about CVSSv4 before it was cool.

Well, CVSSv4 isn't cool yet since it's yet to be fully adopted, but in the meantime, I've researched and come up with this talk. I wasn't given the opportunity to win a 'Best Speaker' award yet. However, I published a few blog posts for Checkmarx and am brewing many other initiatives. I'm also currently studying to pass the CEH certification. Contributing to the AppSec Village at RSAC in San Francisco last year. Check.

Beyond the keyboard, you catch me reading, writing, or practicing martial arts. As in cybersecurity, I seek constant learning.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 11:00-12:59 PDT

Title: Activity: Vulnerability Hunt - The Snippets Edition
When: Friday, Aug 9, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 1 - Map

Description:

Put your skills to the test in this challenge and try to find all the vulnerabilities in the code. We have a wide range of challenges, from easy to advanced in various languages. Can you find them all?

SpeakerBio: Mário Leitão-Teixeira

"Vulnerability" is part of my daily vocabulary at Checkmarx, and I never get sick of it. I dub myself a 'self-certified idiot' because I love learning and hatching ideas. So much, that I've made brainstorming a hobby and kickstarted a team initiative to keep us on the pulse of InfoSec. As a result, we have learned about CVSSv4 before it was cool.

Well, CVSSv4 isn't cool yet since it's yet to be fully adopted, but in the meantime, I've researched and come up with this talk. I wasn't given the opportunity to win a 'Best Speaker' award yet. However, I published a few blog posts for Checkmarx and am brewing many other initiatives. I'm also currently studying to pass the CEH certification. Contributing to the AppSec Village at RSAC in San Francisco last year. Check.

Beyond the keyboard, you catch me reading, writing, or practicing martial arts. As in cybersecurity, I seek constant learning.

Return to Index - Add to Google - ics Calendar file

HRV - Sunday - 11:30-11:59 PDT

Title: Advanced Packet Radio Operation
When: Sunday, Aug 11, 11:30 - 11:59 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

Ready to graduate from basic packet? This presentation dives headfirst into the advanced world of packet radio networking. We'll explore routing protocols like NETROM and ROSE, conquer the intricacies of setting up your own packet radio node, and delve into the world of HF packet communication.

SpeakerBio: Jeremy
No BIO available

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 11:45-13:30 PDT

Title: Adventures in Android Triage Collection
When: Friday, Aug 9, 11:45 - 13:30 PDT
Where: LVCC West/Floor 3/W309 - Map

Description:

Are you curious about accessing and collecting triage data from Android devices? I was. This workshop is designed for the defender that doesn't know much about Android or how to access it to collect forensic triage data, but would like to understand the subject better. This workshop gives a solid foundation for accessing Android devices and collecting data from them. It will cover:

- Installing and using an Android emulator
- How does an Android emulator differ from an actual Android device
- Using the Android Debug Bridge (ADB) to send commands to Android
- Collecting triage data using ADB or natively on the Android device
- Side loading and running a Linux executable on an Android device
- Remote access to the Android native AChoirX collector over TCP
- Collecting triage data both locally and remotely
- Transferring the collected data using ADB, SFTP, and S3
- Things to look out for. Android is very different from Windows, MacOS, and Linux
- Limitations and caveats

This workshop requires Windows 10 or 11. We will install and play with Android Studio, install and play with ADB, and run AChoirX collections both remotely and locally. It is highly recommended that the student come to the workshop with Android Studio, ADB, and AChoirX already installed on their machine. We will make a small amount of time to install the software, but will not be able to troubleshoot any installation issues.

After discovering that the Android Operating System commands nearly 44% of the total Operating Systems market (Windows is about 27%). I set about to see if the AChoirX triage collection program could run on it. Since Android is a Linux variant, and AChoirX already ran on Windows, MacOS, and Linux, it seemed very likely that I could make it work.

In a short time I went from knowing nearly nothing about Android to creating both a remote and local triage collector for Android. This workshop will walk the student through how I created both remote and local triage collection systems for Android. It does not cover analysis of the artifacts, but will cover how to collect data from an Android device (and the limitations) using Free and Open Source tools.

SpeakerBio: Omenscan

No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 10:00-10:59 PDT

Title: Adversarial AI: Disrupting Artificial Intelligence with Style
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:
Speakers: Chloé Messdaghi,Sebastian Cesario,Kasimir Schulz

SpeakerBio: Chloé Messdaghi, Head of Threat Intelligence at HiddenLayer

Chloé Messdaghi is the Head of Threat Intelligence at HiddenLayer, leading efforts to secure AI measures and promote industry-wide security practices. A sought-after public speaker and trusted authority for journalists, her expertise has been widely featured in the media. Recognized as a Power Player by Business Insider and SC Media, Chloé has made significant contributions to cybersecurity. Outside of work, she is dedicated to philanthropy, advancing industry progress, and promoting societal and environmental well-being.

Chloé Messdaghi serves as the Head of Threat Intelligence at HiddenLayer, where she spearheads efforts to fortify security for AI measures and fosters collaborative initiatives to enhance industry-wide security practices for AI. A highly sought-after public speaker and trusted authority for national and sector-specific journalists, Chloé's expertise has been prominently featured across various media platforms. Her impactful contributions to cybersecurity have earned her recognition as a Power Player by esteemed publications such as Business Insider and SC Media.Beyond her professional endeavors, Chloé remains passionately committed to philanthropy aimed at advancing industry progress and fostering societal and environmental well-being.

SpeakerBio: Sebastian Cesario, CTO & Co Founder, BforeAI
No BIO available
SpeakerBio: Kasimir Schulz, Principal Security Researcher at HiddenLayer

Kasimir Schulz, Principal Security Researcher at HiddenLayer, is a leading expert in uncovering zero-day exploits and supply chain vulnerabilities in AI. His work has been featured in BleepingComputer and Dark Reading, and he has spoken at conferences such as FS-ISAC and Black Hat. Kasimir leads the development of advanced tools for automating vulnerability detection and implementing large-scale patches, fortifying systems against supply chain attacks. His dedication to proactive defense measures sets a new standard in cybersecurity resilience.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 13:00-13:50 PDT

Title: Adversary Simulation: Using Blue Eyes to See Red
When: Friday, Aug 9, 13:00 - 13:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

In this session, we'll translate PCAPs, STIX objects, or detection repositories into attack scenarios and send test data to a data lake/SIEM to test detection logic and organizational context. We'll write scenarios in descriptive language, and give public access to a bunch of scenario content for participants to use and contribute to, as well as leave with the data to test your environment with at home if you want, and public access to the free tools to use scenarios.

Speakers: Fred Wilmot,Sebastien Tricaud

SpeakerBio: Fred Wilmot
No BIO available
SpeakerBio: Sebastien Tricaud
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 10:00-17:59 PDT

Title: Adversary simulator and purple teaming hands-on booth
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

Adversary Simulator booth is a volunteer assisted activity, which has hands-on adversary emulation plans and exercises specific to a wide variety of threat-actors; these are meant to provide the participants with a better understanding of adversarial attack emulation. The booth will be hosting a simulated environment meant to recreate enterprise infrastructure, operational technology environment, which serves targets for various attack simulations.The hands-on simulator booth also hosts an activity, which would need the participants to generate their own adversary emulation plans to assess the efficacy of the defense systems based on publicly available cyber threat intelligence.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Sunday - 10:00-11:59 PDT

Title: Adversary simulator and purple teaming hands-on booth
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

Adversary Simulator booth is a volunteer assisted activity, which has hands-on adversary emulation plans and exercises specific to a wide variety of threat-actors; these are meant to provide the participants with a better understanding of adversarial attack emulation. The booth will be hosting a simulated environment meant to recreate enterprise infrastructure, operational technology environment, which serves targets for various attack simulations.The hands-on simulator booth also hosts an activity, which would need the participants to generate their own adversary emulation plans to assess the efficacy of the defense systems based on publicly available cyber threat intelligence.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 10:00-17:59 PDT

Title: Adversary simulator and purple teaming hands-on booth
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

Adversary Simulator booth is a volunteer assisted activity, which has hands-on adversary emulation plans and exercises specific to a wide variety of threat-actors; these are meant to provide the participants with a better understanding of adversarial attack emulation. The booth will be hosting a simulated environment meant to recreate enterprise infrastructure, operational technology environment, which serves targets for various attack simulations.The hands-on simulator booth also hosts an activity, which would need the participants to generate their own adversary emulation plans to assess the efficacy of the defense systems based on publicly available cyber threat intelligence.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 10:00-10:59 PDT

Title: Adversary Village keynote kick-off panel
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:
Speakers: Abhijith “Abx” B R,Bryson Bort ,Ken Kato,Vivek Ramachandran,Sanne Maasakkers

SpeakerBio: Abhijith “Abx” B R

Abhijith B R, also known by the pseudonym Abx, has more than a decade of experience in the offensive cyber security industry. Currently he is involved with multiple organizations as a consulting specialist, to help them build offensive security operations programs, improve their current security posture, assess cyber defense systems, and bridge the gap between business leadership and cyber security professionals. Abhijith’s professional exposure is stretched across multiple industries and various other sectors.

As the founder of Adversary Village, Abhijith spearheads a community driven initiative exclusively focused on adversary simulation, adversary tactics, purple teaming, threat-actor/ransomware research-emulation, and offensive security-adversary tradecraft.

SpeakerBio: Bryson Bort
No BIO available
SpeakerBio: Ken Kato, VP at Omni Federal

Breaking up bureaucracy since 2008, Ken Kato is a leader in large-scale digital transformation for highly regulated industries. It’s his belief that success comes from changing how teams work with each other toward a common goal. Whether it’s an austere data center with bare-metal servers, global-scale cloud deployments, or terrestrial networking in the far reaches of space, it always comes back to the people.

Ken’s recent accomplishments include: being a founding member of USAF Kessel Run, the first federal software factory; building Black Pearl, the Navy’s premiere DevSecOeps platform; and working with the White House to secure and scale critical cyber-infrastructure. But technology alone can’t solve complex problems. With this in mind, Ken balances his years of experience with industry data to develop sustainable strategies for organizational growth and predict how decisions made today will be survivable in the years ahead.

SpeakerBio: Vivek Ramachandran, Founder at SquareX

Vivek Ramachandran is a security researcher, book author, speaker-trainer, and serial entrepreneur with over two decades of experience in offensive cybersecurity. He is currently the founder of SquareX, building a browser-native security product focused on detecting, mitigating, and threat-hunting web attacks against enterprise users and consumers. Prior to that, he was the founder of Pentester Academy (acquired in 2021), which has trained thousands of customers from government agencies, Fortune 500 companies, and enterprises from over 140+ countries. Before that, Vivek’s company built an 802.11ac monitoring product sold exclusively to defense agencies. Vivek discovered the Caffe Latte attack, broke WEP Cloaking, conceptualized enterprise Wi-Fi Backdoors, and created Chellam (Wi-Fi Firewall), WiMonitor Enterprise (802.11ac monitoring), Chigula (Wi-Fi traffic analysis via SQL), Deceptacon (IoT Honeypots), among others. He is the author of multiple five-star-rated books in offensive cybersecurity, which have sold thousands of copies worldwide and have been translated into multiple languages. He has been a speaker/trainer at top security conferences such as Blackhat USA, Europe and Abu Dhabi, DEFCON, Nullcon, Brucon, HITB, Hacktivity, and others. Vivek’s work in cybersecurity has been covered in Forbes, TechCrunch, and other popular media outlets. In a past life, he was one of the programmers of the 802.1x protocol and Port Security in Cisco’s 6500 Catalyst series of switches. He was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. He has also published multiple research papers in the field of

DDoS, ARP Spoofing Detection, and Anomaly-based Intrusion Detection Systems. In 2021, he was awarded an honorary title of Regional Director of Cybersecurity by Microsoft for a period of three years, and in 2024 he joined the BlackHat Arsenal Review Board.

SpeakerBio: Sanne Maasakkers, Threat Intel at Mandiant
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Adversary Wars CTF
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05 - Map

Description:

Adversary Village proudly presents "Adversary Wars CTF", an official contest at DEF CON, where the participants will have to pose as adversaries and replicate adversarial actions against each element of a “target” organization. Adversary Wars would have real world simulation of CTF scenarios and challenges, where the participants can perform various attacks and learn new attack vectors, TTPs, techniques, etc. To visualize the CTF environment, the contest area will feature a miniature model of the city made using interlocking-plastic-bricks. The breached components OR organization buildings will be physically marked in the city model as the CTF progresses.

We are excited to be back at DEF CON as an official contest this year. Adversary Wars CTF will be located in the contest area for DEF CON 32.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Adversary Wars CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05 - Map

Description:

Adversary Village proudly presents "Adversary Wars CTF", an official contest at DEF CON, where the participants will have to pose as adversaries and replicate adversarial actions against each element of a “target” organization. Adversary Wars would have real world simulation of CTF scenarios and challenges, where the participants can perform various attacks and learn new attack vectors, TTPs, techniques, etc. To visualize the CTF environment, the contest area will feature a miniature model of the city made using interlocking-plastic-bricks. The breached components OR organization buildings will be physically marked in the city model as the CTF progresses.

We are excited to be back at DEF CON as an official contest this year. Adversary Wars CTF will be located in the contest area for DEF CON 32.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Adversary Wars CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05 - Map

Description:

Adversary Village proudly presents "Adversary Wars CTF", an official contest at DEF CON, where the participants will have to pose as adversaries and replicate adversarial actions against each element of a “target” organization. Adversary Wars would have real world simulation of CTF scenarios and challenges, where the participants can perform various attacks and learn new attack vectors, TTPs, techniques, etc. To visualize the CTF environment, the contest area will feature a miniature model of the city made using interlocking-plastic-bricks. The breached components OR organization buildings will be physically marked in the city model as the CTF progresses.

We are excited to be back at DEF CON as an official contest this year. Adversary Wars CTF will be located in the contest area for DEF CON 32.

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 10:00-17:59 PDT

Title: Adversary-Adventure Table-top Game
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

Adversary Adventure is a Choose-Your-Own-Adventure model interactive table-top exercise game, where everyone can participate and choose various tasks. The participants can choose to play as an attacker who performs adversarial activities against a target, a defender who deals with a potential breach, as a CISO who is managing a ransomware attack, or even as management executives going through a table-top exercise.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Sunday - 10:00-11:59 PDT

Title: Adversary-Adventure Table-top Game
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

Adversary Adventure is a Choose-Your-Own-Adventure model interactive table-top exercise game, where everyone can participate and choose various tasks. The participants can choose to play as an attacker who performs adversarial activities against a target, a defender who deals with a potential breach, as a CISO who is managing a ransomware attack, or even as management executives going through a table-top exercise.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 10:00-17:59 PDT

Title: Adversary-Adventure Table-top Game
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

Adversary Adventure is a Choose-Your-Own-Adventure model interactive table-top exercise game, where everyone can participate and choose various tasks. The participants can choose to play as an attacker who performs adversarial activities against a target, a defender who deals with a potential breach, as a CISO who is managing a ransomware attack, or even as management executives going through a table-top exercise.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Advocating for an Inclusive Cyber-Civil Rights Policy Agenda for Vulnerable Communities
When: Friday, Aug 9, 14:00 - 14:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

Cyber-financial crimes devastate marginalized communities, robbing them of economic opportunity and hard earned civil rights. This panel issues an urgent call to action to cyber advocates: join forces in pioneering policy solutions that enhance community resilience against these persistent threats to our global community. Our experts go beyond critiquing existing laws to envision groundbreaking models prioritizing the voices of impacted groups. We'll explore how to effectively amplify grassroots initiatives fostering digital awareness and empowerment from the ground up. This is a roadmap for multi-stakeholder collaboration - uniting policy leaders, corporate innovators, government officials, hackers, and advocates. Together we can build robust frameworks that embed civil rights into the core of cybersecurity strategy and implementation.

Speakers: Nicole Tisdale,Kemba Walden,Jacob H Braun,Elizabeth Eigner

SpeakerBio: Nicole Tisdale, Founder at Advocacy Blueprints

Nicole Tisdale is a fifteen-year national security expert and former Director at The White House - National Security Council and the U.S. Congress' House Committee on Homeland Security. Nicole's policy expertise encompasses cybersecurity, counterintelligence, and election security. Nicole founded Advocacy Blueprints, a policy consulting and advocacy training firm. Her creation and commitment cyber-impact policy is evidenced by her writing The Hidden Injustice of Cyberattacks for WIRED Magazine and her commitment to civic engagement for advocates highlighted in her book "Right to Petition." She serves in several advisor and fellowship positions, including Aspen Digital, POPVOX Foundation, and Omidyar Networks.

SpeakerBio: Kemba Walden, President at Paladin Global Institute

Kemba Walden is President of the Paladin Global Institute and former Acting National Cyber Director at the White House Office of the National Cyber Director (ONCD). Kemba also served a decade at the Department of Homeland Security (DHS) and three years at Microsoft. Since 2019, Kemba has been an adjunct professor of information security law and regulatory compliance at Georgetown University's School of Continuing Studies, which she balances with her duties as a member of the Council on Foreign Relations and Atlantic Council Board of Directors, as well as co-chair of the Aspen Digital U.S. Cybersecurity Group.

SpeakerBio: Jacob H Braun, Acting Principal Deputy National Cyber Director at Office of the National Cyber Director (ONCD)

Jake Braun served in the White House as Acting Principal Deputy National Cyber Director from May 2023 to July 2024. Prior to joining the White House Office of the National Cyber Director, he was appointed by President Joseph Biden as Senior Counselor to the Secretary of Homeland Security. Braun is also a lecturer at the University of Chicago's Harris School of Public Policy Studies and Chairman of the Cyber Policy Initiative there.

From 2009 to 2011, Braun served as White House Liaison to the U.S. Department of Homeland Security. Braun is also co-founder of the DEF CON Voting Machine Hacking Village (Voting Village) hacker conference."

SpeakerBio: Elizabeth Eigner, Security Policy Strategist at Microsoft

Elizabeth Eigner is a Security Policy Strategist in Microsoft's Global Cybersecurity Policy, where she oversees its marginalized user protection initiatives, tailoring Microsoft's cybersecurity approach to the needs of marginalized communities. Elizabeth also leads Microsoft's High-risk User and Human Rights Defender Protection initiative. Prior to

joining Microsoft, Elizabeth worked at the Washington Technology Industry Association (WTIA), where she provided policy and strategic guidance on expanding digital access to underserved Washington communities, and MIT Solve, Massachusetts Institute of Technology's social impact accelerator, where she collaborated with tech-based social entrepreneurs around the world solving challenges related to digital inclusion and equity.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 13:00-14:59 PDT

Title: AI Art Battle
When: Friday, Aug 9, 13:00 - 14:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

Welcome to the “AI Art Battle" Generative AI Art Contest!

This unique competition invites creative minds to dive into the world of artificial intelligence and art. The challenge is to craft the most imaginative prompts that will be used by generative AI models to create artwork.

Contestants will not be creating the art themselves; instead, they will focus on designing prompts for well-known topics that push the boundaries of creativity and innovation.

How It Works:

Select a Topic: Contestants will choose from a list of random topics.

These could range from historical events, famous literary works, mythical creatures, futuristic landscapes, to iconic pop culture references.

Craft a Prompt:

Using their creativity, contestants will write a detailed prompt designed to guide AI models in generating original artwork. The prompts should be clear, imaginative, and offer enough detail to spark the AI's artistic capabilities.

Submission: Each contestant will submit their prompt and the intended outcome.

AI Generation: The submitted prompts will be fed into a generative AI art model, which will create corresponding artworks based on the prompts.

A random panel will determine who the winners are.

Schedule: - 13:00 - 13:30 setup - 13:30 - 14:00 qualifiers - 14:00 - 15:00 contest

Return to Index - Add to Google - ics Calendar file

AIV - Friday - 16:00-16:59 PDT

Title: AI Village Day 1 Keynote – Poison, injection, evasion, oh my! Grounding AI security threats in data driven reality
When: Friday, Aug 9, 16:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Christina will speak to the latest MITRE ATLAS community efforts focused on capturing and sharing cross community data on real world AI incidents, expanding the community's data on vulnerabilities that can arise when using open-source AI models or data, especially for vulnerabilities that fall outside of the scope of CVE/CWE, and developing mitigations to defend against these AI security threats and vulnerabilities.

MITRE ATLAS () is a public knowledge base of adversary tactics and techniques based on real-world attack observations and realistic demonstrations from artificial intelligence (AI) red teams and security groups. There are a growing number of vulnerabilities in AI-enabled systems as the incorporation of AI increases the attack surfaces of existing systems beyond those of traditional cyberattacks. We developed ATLAS to raise community awareness and readiness for these unique threats, vulnerabilities, and risks in the broader AI assurance landscape.

SpeakerBio: Christina Liaghati
No BIO available

Return to Index - Add to Google - ics Calendar file

AIV - Saturday - 10:00-17:59 PDT

Title: AI Village Demos
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Join us at the AI Village for interactive demonstrations at the intersection of AI and security. Attempt to hijack and manipulate autonomous robots using large language models and generative AI. Fool your friends by creating deep fakes with a state-of-the-art setup from Bishop Fox, complete with DSLR camera, green screen, and props. Finally, put your social engineering awareness to the test with DARPA's deep fake analysis system, designed to identify and attribute manipulated and synthetic media. Don't miss this opportunity to engage with adversarial AI technologies and learn about their implications on the future, at DEF CON 32!

Return to Index - Add to Google - ics Calendar file

AIV - Sunday - 10:00-12:59 PDT

Title: AI Village Demos
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Join us at the AI Village for interactive demonstrations at the intersection of AI and security. Attempt to hijack and manipulate autonomous robots using large language models and generative AI. Fool your friends by creating deep fakes with a state-of-the-art setup from Bishop Fox, complete with DSLR camera, green screen, and props. Finally, put your social engineering awareness to the test with DARPA's deep fake analysis system, designed to identify and attribute manipulated and synthetic media. Don't miss this opportunity to engage with adversarial AI technologies and learn about their implications on the future, at DEF CON 32!

Return to Index - Add to Google - ics Calendar file

AIV - Friday - 10:00-17:59 PDT

Title: AI Village Demos
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Join us at the AI Village for interactive demonstrations at the intersection of AI and security. Attempt to hijack and manipulate autonomous robots using large language models and generative AI. Fool your friends by creating deep fakes with a state-of-the-art setup from Bishop Fox, complete with DSLR camera, green screen, and props. Finally, put your social engineering awareness to the test with DARPA's deep fake analysis system, designed to identify and attribute manipulated and synthetic media. Don't miss this opportunity to engage with adversarial AI technologies and learn about their implications on the future, at DEF CON 32!

Return to Index - Add to Google - ics Calendar file

TCV - Saturday - 10:00-10:59 PDT

Title: AI-Driven Cyber Resilience: Surviving the 5G Threat Landscape
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

This panel discussion will delve into the critical intersection of artificial intelligence and cybersecurity in the context of the rapidly evolving 5G network environment. By bringing together experts in AI, 5G network security, and AI-driven solutions

Speakers: Shina Liu,Niklas Lindroos,Ezz Tahoun,Akib Sayyed

SpeakerBio: Shina Liu

Shina Liu has over two decades of experience in the telecom industry, beginning as a software developer for 3G networks. Since receiving her CISSP certification in 2007, she led product security verification for 4G and 5G networks and currently serve as a senior security analyst. Based in Naperville, she is a member of Nokia's Technical Leadership Council Committee and has been actively involved in ML/AI/GenAI initiatives since 2019.

SpeakerBio: Niklas Lindroos, Head of PSIRT and Advanced Security Testing lab at Nokia Corporation

Niklas is the Head of PSIRT and Advanced Security Testing lab - the red and blue teams of Nokia Corporation. He and his team manage the response to serious vulnerabilities and incidents in telecommunication networks globally and conduct security simulations and testing of essential network functions. He has over 30 years of experience in network and telecommunications security.

SpeakerBio: Ezz Tahoun

Ezz Tahoun, a distinguished cyber-security data scientist, who won AI & innovation awards at Yale, Princeton and Northwestern. He also got innovation awards from Canada’s Communications Security Establishment, Microsoft US, Trustwave US, PIA US, NATO, and more. He ran data science innovation programs and projects for OrangeCyber Defense, Forescout Technologies, Royal bank of Canada, Governments, and Huawei Technologies US. He has published 20 papers, countless articles and 15 open source projects in the domain. When he was 19 years old he started his CS PhD in one of the top 5 labs in the world for cyber & AI, in the prestigious University of Waterloo, where he published numerous papers and became a reviewer for top conferences. His designations include: SANS/GIAC-Advisory-Board, aCCISO, CISM, CRISC, GCIH, GFACT, GSEC, CEH, GCP-Professional-Cloud-Architect, PMP, BENG and MMATH. He was an adjunct professor of cyber defense and warfare at Toronto’s school of management.

SpeakerBio: Akib Sayyed, Founder and Director at Matrix Shell Technologies

Akib, Founder and Director of Matrix Shell Technologies, has over 12 years of experience in Telecom Security. He has served diverse telecom operators across India, Africa, and the Middle East, specializing in signaling protocols and technologies like GSM, UMTS, LTE, 5G, and VoLTE. He has led numerous penetration testing projects, disclosed a GSM vulnerability in 2012, and worked with various open-source telecom platforms. Akib has also delivered training at Black Hat and DEFCON, contributing significantly to the cybersecurity community. His education includes a Bachelor's in Engineering (CSE) and certifications in ISO 17025:2017 and 5G.

Return to Index - Add to Google - ics Calendar file

AIV - Friday - 13:30-14:30 PDT

Title: AI'll be watching you. Greybox Attacks against an Embedded AI
When: Friday, Aug 9, 13:30 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

AI'll be watching you will cover attacking an embedded AI on a family of popular security cameras with over 100,000 combined reviews on Amazon. The camera's embedded AI system is used for on-device person detection, a system that filters notifications based on whether a person is detected. Traditionally the camera would alert the owner if any motion was detected, meaning that an attacker would have to have no motion be detected, but now with the embedded AI making decisions, an attacker needs to only appear not to be human. While this may seem a simple task, dressing up as a giant bush would be noticeable by the people around the attacker, meaning that a successful attack against this system requires the on-camera AI to be tricked while not alerting nearby people to any suspicious disguises.

In this talk we will cover the steps we took to research and gain access to the device in order to perform greybox attacks against its embedded AI. We will demonstrate how we rooted an older version of the device to gain access to how the models were brought to the camera. We will show how the knowledge we gained while reverse engineering let us download the models for any arbitrary device or firmware and, eventually, how we were able to exploit and gain root on the newer, more secure device. We will show the audience our process in which we discovered and reverse-engineered a proprietary model format that we had never seen before. Finally, we will show how, once we understood the model, we were able to perform attacks against both it and the camera.

The purpose of this talk is to raise awareness about the insecurity of embedded AI as well as to demonstrate how known attack techniques can be used on never-before-seen models, showcasing that AI/ML research has truly passed the infant stage and has reached a point where developed methods can be broadly applied.

Speakers: Ryan Tracey,Kasimir Schulz,Tom Boner

SpeakerBio: Ryan Tracey, HiddenLayer
No BIO available
SpeakerBio: Kasimir Schulz, Principal Security Researcher at HiddenLayer

Kasimir Schulz, Principal Security Researcher at HiddenLayer, is a leading expert in uncovering zero-day exploits and supply chain vulnerabilities in AI. His work has been featured in BleepingComputer and Dark Reading, and he has spoken at conferences such as FS-ISAC and Black Hat. Kasimir leads the development of advanced tools for automating vulnerability detection and implementing large-scale patches, fortifying systems against supply chain attacks. His dedication to proactive defense measures sets a new standard in cybersecurity resilience.

SpeakerBio: Tom Boner, HiddenLayer
No BIO available

Return to Index - Add to Google - ics Calendar file

BICV - Sunday - 10:30-12:30 PDT

Title: Ain’t that a Breach: Zero Trust Is the Only Solution!
When: Sunday, Aug 11, 10:30 - 12:30 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Living a life devoid of trust in anything or anyone can lead to a dismal existence. However, in the realm of cyber security, embracing the concept of Zero Trust is essential. Trust was never meant for networks and is now irrelevant in the digital realm. This discussion explores why trust has become a vulnerability and underscores the importance for organizations to adopt principles such as Zero Trust to effectively respond to the ever-changing threat landscape; failure to do so may lead to their extinction within a few years.

SpeakerBio: Dr. Louis DeWeaver III, Cyber Security Consultant at Marsh McLennan Agency

Dr. Louis DeWeaver is a Cyber Security Consultant at Marsh McLennan Agency (MMA). With over 20 years of experience, Louis provides strategic direction to the organization and its clients in developing and implementing effective cyber strategies and initiatives. He strives to stay up to date on the latest cyber security trends and continuously identifies the evolving methods used by attackers.

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 20:00-23:59 PDT

Title: AIV + BTV Pool Party featuring DUNK-A-FED
When: Saturday, Aug 10, 20:00 - 23:59 PDT
Where: Other / See Description

Description:

The AI Village and Blue Team Village Pool Party will feature free tacos, cash bars, sponsor cabanas, with entertainment by DJ R.O.C.K.M.A.N. and "Dunk A Fed" benefitting Blacks in Cyber and Women in Security and Privacy. Sahara Azilo Pool, Saturday, August 10, 8pm to midnight. DEF CON badge required for entry. All ages. Visit Blacks In Cyber Village or WISP at DEF CON for your Dunk A Fed raffle ticket.

Return to Index - Add to Google - ics Calendar file

Title: AIxCC Closing Ceremonies
When: Sunday, Aug 11, 12:30 - 13:15 PDT
Where: LVCC West/Floor 1/Hall 1/Tracks 1-2 - Map

Description:

DARPA and ARPA-H joined forces for the AI Cyber Challenge (AIxCC), a two-year competition aimed at revolutionizing cybersecurity through AI-driven solutions. AIxCC asks the nation's top talent in AI and cybersecurity to develop Cyber Reasoning Systems capable of automatically finding and fixing software vulnerabilities to secure critical software. In this talk, we are excited to announce the results of the Semifinals event. We will conduct a brief examination of the AI systems developed by the top teams by analyzing their strategies, discuss key innovations and methodologies employed, and discuss the overall impact of the competition on the cybersecurity landscape. The top-ranking teams will be eligible to win one of the $2 million in semifinal prizes, as well as a spot in the Finals competition at DEF CON 33.

Speakers: Andrew Carney,Perri Adams

SpeakerBio: Andrew Carney, Program Manager at Advanced Research Projects Agency for Health (ARPA-H)

Andrew Carney joined ARPA-H in July 2023 from HSBC's Cybersecurity Science and Analytics group, where he worked as a principal researcher. He has over 15 years of experience in software and hardware vulnerability research, technical education and training, and management of research and development teams.

In addition to his role as program manager with ARPA-H, Carney holds a joint program manager appointment with the Defense Advanced Research Projects Agency (DARPA) for the AI Cyber Challenge (AIxCC), a competition focused on securing software in critical infrastructure. Before HSBC, Carney was a technical advisor and contractor for the Defense Advanced Research Projects Agency (DARPA). At DARPA, he supported research efforts focused on reverse engineering, program analysis, human-machine teaming, and automated program repair. Throughout his career, Carney has been involved in competitive hacking (called Capture the Flag, or CTF) as both a player and a competition organizer. He holds a master's degree in computer science from The Johns Hopkins University.

SpeakerBio: Perri Adams, Special Assistant to the Director at Defense Advanced Research Projects Agency (DARPA)

Ms. Perri Adams is a special assistant to the director at DARPA, where she advises stakeholders at the agency and across the U.S. government on the next generation of AI and cybersecurity technology.

Prior to this role, Adams was a program manager within DARPA's Information Innovation Office (I2O), where, among other programs, she created the AI Cyber Challenge (AIxCC).

Adams has been an avid participant in cybersecurity CTF competitions and was one of the organizers of the DEF CON CTF. She holds a bachelor's degree in computer science from Rensselaer Polytechnic Institute and is a proud alumna of the computer security club, RPISEC.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: All content areas generally open
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: All content areas generally open
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: All content areas generally open
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West - Map

Description:

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 13:00-13:59 PDT

Title: All Your Keyboards Are Belong to US!
When: Saturday, Aug 10, 13:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

This is a live tutorial of hacking against keyboards of all forms. Attacking the keyboard is the ultimate strategy to hijack a session before it is encrypted, capturing plaintext at the source and (often) in much simpler ways than those required to attack network protocols.

In this session we explore available attack vectors against traditional keyboards, starting with plain old keyloggers. We then advance to "Van Eck Phreaking" style attacks against individual keystroke emanations as well as RF wireless connections, and we finally graduate to the new hotness: acoustic attacks by eavesdropping on the sound of you typing!

Use your newfound knowledge for good, with great power comes great responsibility!

A subset of signal leak attacks focusing on keyboards. This talk is compiled with open sources, no classified material will be discussed.

SpeakerBio: Federico Lucifredi, Product Management Director, Ceph Storage at IBM and Red Hat

Federico Lucifredi is the Product Management Director for Ceph Storage at IBM and Red Hat and a co-author of O'Reilly's "Peccary Book" on AWS System Administration. Previously, he was the Ubuntu Server product manager at Canonical, where he oversaw a broad portfolio and the rise of Ubuntu Server to the rank of most popular OS on Amazon AWS. A software engineer-turned-manager at the Novell corporation, he was part of the SUSE Linux team, overseeing the update lifecycle and delivery stack of a $150 million maintenance business. A CIO and a network software architect at advanced technology and embedded Linux startups, Federico was also a lecturer for over 200 students in Boston University's graduate and undergraduate programs, and simultaneously a consultant for MIT implementing fluid-dynamics simulations in Java.

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 11:30-12:30 PDT

Title: AMA on Proxmark3 with Iceman
When: Saturday, Aug 10, 11:30 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:
SpeakerBio: Iceman
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 12:30-13:15 PDT

Title: AMD Sinkclose: Universal Ring -2 Privilege Escalation
When: Saturday, Aug 10, 12:30 - 13:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

System Management Mode (SMM) is one of the most powerful execution modes in the x86 architecture and code at this level is invisible to the Hypervisor and OS-level protections, including anti-cheat engines and anti-virus systems. While the BIOS ecosystem's complexity has led to a multitude of vulnerabilities in firmware over time, vendors are now making strides in delivering patches with greater speed and efficiency. Unfortunately, these efforts are not enough in the presence of a CPU vulnerability.

When researching the AMD processor, our team noticed a flaw in one of the critical components required for securing SMM. This silicon-level issue appears to have remained undetected for nearly two decades.

This presentation starts by providing an introduction to SMM and the security mechanisms that the AMD processor provides to support it. Subsequently, it delves into the CPU design flaw and the complete methodology and engineering used to create a universal ring -2 privilege escalation exploit.

Speakers: Enrique Nissim,Krzysztof Okupski

SpeakerBio: Enrique Nissim, Principal Security Consultant at IOActive

Enrique Nissim is a security engineer with over a decade of professional experience working on vulnerability research. As a Principal Security Consultant at IOActive, he is mainly involved in projects requiring a deep understanding of operating systems, CPU architectures, embedded firmware and software development. Over his career, Enrique has delivered multiple presentations at several leading events including Black Hat USA, CansecWest, Ekoparty, ZeroNights and Hardwear.io.

SpeakerBio: Krzysztof Okupski, Associate Principal Security Consultant at IOActive

Krzysztof Okupski is an Associate Principal Security Consultant with IOActive where he specialises in embedded security. While he enjoys hacking various targets, he is particularly interested in the nitty-gritty details of platform security where small misconfigurations can lead to critical issues.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 14:00-14:59 PDT

Title: Amenaza persistente: UXHIL y la propagación de URSA
When: Friday, Aug 9, 14:00 - 14:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Esta conferencia se centrará en el actor amenaza UXHIL, responsable de la distribución del malware URSA, ofreciendo una visión profunda basada en ciberinteligencia. Exploraremos cómo este actor ha estado distribuyendo el malware, las tácticas, técnicas y procedimientos (TTPs) que utiliza y cómo es su cadena de infección. Los asistentes aprenderán a identificar y analizar estos patrones para desarrollar estrategias efectivas de mitigación.

Speakers: Jesika Juarez,Armando Aguilar

SpeakerBio: Jesika Juarez, Senior Cyber Threat Intelligence Analyst at Deloitte México

Jesika Juarez es una analista con casi cinco años de experiencia en el campo de inteligencia de amenazas en el equipo de Cyber Threat Intelligence en Deloitte México. Especializada en análisis de malware, investigación forense y técnicas de OSINT (Open Source Intelligence), ha desempeñado un papel crucial en la identificación, análisis y mitigación de amenazas cibernéticas avanzadas. Jesika es egresada de la Facultad de Estudios Superiores Aragón de la carrera de Ingeniería en Computación, la cual cuenta con una certificación de Malware Analysis y Digital Forensics impartidas por Elearnsecurity

SpeakerBio: Armando Aguilar, Cyber Threat Analyst

Armando Aguilar es un analista de inteligencia de ciberamenazas con más de 6 años de experiencia en la identificación, análisis y mitigación de amenazas que se encuentran afectado a México y Latinoamérica. Actualmente, es miembro del equipo de Threat Intelligence en una de las instituciones financieraa más grandes de México.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 11:00-11:30 PDT

Title: An adversarial approach to Airline Revenue Management Proving Ground
When: Friday, Aug 9, 11:00 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Richard Branson is oft quoted with the quip that the quickest way to become a millionaire in the Airline Industry is to start as a billionaire. An Industry constrained by high fixed capital costs, bi-lateral capacity treaties, airport slots and curfews, labour etc; Airlines use the practice of revenue management to fill planes, maximise earnings and keep competitors at bay. But you're not interested in an economics talk – this is a hacker con. I'm here to provide a birds-eye view and introduction into how fares and ticketing work, debunking some myths while outlining system constraints and limitations that introduce vulnerabilities. As an outcome, attendees should gain an introductory understanding of airline industry pricing, published fares and terminology. With most blogged 'deals' patched quicker than RCEs, the deeper understanding of not what but how, facilitates a progression for those interested to interact on more specialised discussion forums.

SpeakerBio: Craig Lester
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 13:00-14:50 PDT

Title: An Operator's Guide: Hunting SCCM in the Real World
When: Saturday, Aug 10, 13:00 - 14:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

SCCM abuse has become a popular technique in the offensive security community but can be intimidating to test in production environments due to its complexity. This workshop aims to provide operators not only a safe environment to practice tradecraft but also provide them with the confidence to properly find and assess SCCM during their engagements.

Speakers: Garrett Foster,Zachary Stein

SpeakerBio: Garrett Foster, Senior Consultant at SpecterOps

Garrett Foster (@garrfoster) is a Senior Consultant at SpecterOps, where he conducts red team operations, penetration testing, research, training, and course development. Garrett has presented at WWHF and BsidesPDX. Garrett is a the primary author of SCCMHunter and a co-author of Misconfiguration Manager.

SpeakerBio: Zachary Stein
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 16:00-16:30 PDT

Title: Analyzing the Security of Satellite-Based Air Traffic Control
When: Friday, Aug 9, 16:00 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Automatic Dependent Surveillance – Contract (ADS-C) is a satellite-based aviation datalink application used to monitor aircraft in remote regions. It is a crucial method for air traffic control to track aircraft where other protocols such as ADS-B lack connectivity. Even though it has been conceived more than 30 years ago, and other legacy communication protocols in aviation have shown to be vulnerable, ADS-C's security has not been investigated so far in the literature. We conduct a first investigation to close this gap. First, we compile a comprehensive overview of the history, impact, and technical details of ADS-C and its lower layers. Second, we build two software-defined radio receivers in order to analyze over 120'000 real-world ADS-C messages. We further illustrate ADS-C's lack of authentication by implementing an ADS-C transmitter, which is capable of generating and sending arbitrary ADS-C messages. Finally, we use the channel control offered through a software-defined ADS-C receiver and transmitter as a basis for an in-depth analysis of the protocol weaknesses of the ADS-C system. The found vulnerabilities range from passively tracking aircraft to actively altering the position of actual aircraft through attacks on the downlink and the uplink. We assess the difficulty and impact of these attacks and discuss potential countermeasures.

We will further look at satellite-based ADS-B receivers and discuss their security and how they relate to ADS-C.

SpeakerBio: Martin Strohmeier, Senior Scientist at Cyber Defence Campus

Martin Strohmeier is a Senior Scientist at the Swiss Cyber Defence Campus, where he is responsible for vulnerability research programmes into aircraft, satellites and cars. His work was published in all major systems security conferences, totalling more than 100 publications to date. He has also spoken previously at the DEFCON Aerospace Village and co-organized CTFs there.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 15:00-15:45 PDT

Title: Android App Usage and Cell Tower Location: Private. Sensitive. Available to Anyone?
When: Friday, Aug 9, 15:00 - 15:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Do you consider the list of mobile apps you use and the frequency at which you use them private information? What about the GPS coordinates of the cell towers to which your smartphone connects? The Android framework restricts third-party apps from freely obtaining this information – unless the user explicitly grants the app access. Android is a diverse ecosystem that comes with many benefits, but device vendors can still unintentionally expose app usage and device location in a variety of ways. We uncover privacy leaks of both types of data, where pre-loaded vendor software exposes app usage and location to co-located software. We also explore various local exposures of this data, where it is leaked to resources that do not require any special permissions or privileges to access.

We discovered these leakages across several major vendors, including Samsung, Nokia, Transsion brands (i.e., Tecno, Infinix, and Itel), and additional vendors that utilize a pre-installed Qualcomm app for performance monitoring. We cover each of these exposures in detail. App usage reveals the subset of the apps that the user actually interacts with, which can be collected, combined with location data, and analyzed for advertising, profiling, and establishing user pattern-of-life.

1. link
2. link
3. link
4. link
5. link
6. link
7. link
8. link
9. link
10. link
11. link
12. link
13. link
14. link
15. link
16. link
17. link
18. link
19. link
20. link
21. link
22. link
23. link
24. link
25. link

SpeakerBio: Ryan Johnson, Senior Director, R&D at Quokka

Dr. Ryan Johnson is a Senior Director, R&D at Quokka (formerly Kryptowire). His research interests are static and dynamic analysis of Android apps and reverse engineering. He is a co-founder of Quokka and has presented at DEF CON, Black Hat (USA, Asia, & MEA), IT-Defense, and @Hack. His research in Android security has been assigned dozens of CVEs and is responsible for discovering the Adups spyware that affected millions of Android smartphones.

IOTV - Sunday - 12:00-12:59 PDT

Title: Anyone can hack IoT - a beginner's guide to hacking your first IoT device
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Yes, anyone can hack IoT devices and I'll show you how! It doesn't matter if you're an experienced pen tester in other fields, completely new to cybersecurity or just IoT curious, by the end of this talk you'll have the knowledge to hack your first device. You might be thinking - but I thought IoT was complicated, required knowledge of hardware, and expensive tools. In this talk, I'm here to dispel those myths by directly showing you the methodology, tools and tactics you can use to go and hack an IoT device today (or maybe when you get home). I'll cover what IoT devices are best for beginners, what tools you need (and don't need), how to build a small toolkit for **SpeakerBio:** Andrew "DigitalAndrew" Bellini, Instructor at TCM

Andrew Bellini, also known as DigitalAndrew, is an electrical engineer by trade with a bachelor's degree in electrical engineering and a licensed Professional Engineer in Ontario, Canada. He is the creator of TCM Security's Beginner's Guide to IoT and Hardware Hacking course and Practical Junior IoT Tester certification. While his background and most of his career are in electrical engineering, Andrew is also an avid and passionate ethical hacker! In addition to being an instructor at TCM, he is also a longtime student and credits their quality courses helping him transition his career into cybersecurity. Including his love for all things ethical hacking, cybersecurity, CTFs and tech, he's also a dad, plays guitar and is very passionate about the outdoors and fishing!

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 11:00-13:59 PDT

Title: Application Threat Modeling with Trike
When: Saturday, Aug 10, 11:00 - 13:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Classroom - Map

Description:

The earlier we perform security interventions, the better. The best time? While we're designing an application. This workshop will discuss the importance and use of Application Threat Modeling during app design, how to apply it to existing applications during later phases of development, then perform application threat modeling on an example web application using the Trike methodology.

The presented methodology is built on the concept that understanding the design of an application is all that is needed to create a threat model - and doing so can remove the uncertainties and brainstorming that other security threat modeling can require. Rather than requiring a deep security knowledge, all we need is to understand the application - something developers are uniquely suited to do.

SpeakerBio: AreTillery

Tillery (they/them) is a co-founder of Neuvik Solutions and serves as their Director of Training & Education. Tillery has been in formal education and professional training roles for the US Department of Defense as well as for commercial companies for more than a decade. They have spent their career in cybersecurity on both sides of the red/blue divide, first focusing on reverse engineering and exploit development, then bringing their offensive mindset to the field of Application Security. Tillery brings deep technical knowledge and pedagogical training to instruction in cybersecurity, computer science, and mathematics.

Return to Index - Add to Google - ics Calendar file

XRV - Saturday - 11:00-12:59 PDT

Title: AR + Art = interactive installations to bring your stories to life
When: Saturday, Aug 10, 11:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

Learn how in this hands-on lab with resident AR designer, Zaire Moore

SpeakerBio: Zaire Moore, BlackTerminus

Cinematographer | AR Designer | Content Creator

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 21:00-01:59 PDT

Title: Arcade Party
When: Friday, Aug 9, 21:00 - 01:59 PDT
Where: LVCC West/Floor 1/W106-W109-Chillout 1 - Map

Description:

The Arcade Party is back! Come play your favorite classic arcade games while jamming out to Keith Myers DJing. Your favorite custom built 16 player LED foosball table will be ready for some competitive games. This epic party, free for DEF CON 32 attendees to enjoy and play, is hosted by the Military Cyber Professionals Association (a tech ed charity) and friends.

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 14:00-15:59 PDT

Title: Area DC32: An Interactive Tabletop Takes Flight (A BTV Panel)
When: Friday, Aug 9, 14:00 - 15:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

Join BTV and the Aerospace Village for a large-scale interactive tabletop exercise with a game show panel format. Participants will walk through a security incident within input from security pros, tabletop experts, and aerospace insiders. The host will invite answers and prizes may fly through the air as our subject matter experts weigh in on the response effort with snark but no judgment.

Join BTV and the Aerospace Village for a large-scale interactive tabletop exercise with a game show panel format. Participants will walk through a security incident within input from security pros, tabletop experts, and aerospace insiders. The host will invite answers and prizes may fly through the air as our subject matter experts weigh in on the response effort with snark but no judgment.

Speakers: Aakin Patel,Caspian Kilkelly,Gwyddia,Harlan Geer,Shea Nangle,Matt Mayes

SpeakerBio: Aakin Patel
No BIO available
SpeakerBio: Caspian Kilkelly
No BIO available
SpeakerBio: Gwyddia
No BIO available
SpeakerBio: Harlan Geer
No BIO available
SpeakerBio: Shea Nangle
No BIO available
SpeakerBio: Matt Mayes, Aerospace Village
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: ARINC 664 CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

ARINC 664 is an extension to IP networking that adds deterministic QoS for Aircraft Systems over Ethernet. Sit down and learn about how the extensions to 802.3 is used on aircraft, how that flight critical data is transferred in a timely matter, and how to manipulate the data on these networks. This progressive difficulty CTF provides a fun and informative way of approaching ARINC 664 networking.

SpeakerBio: Boeing
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: ARINC 664 CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

ARINC 664 is an extension to IP networking that adds deterministic QoS for Aircraft Systems over Ethernet. Sit down and learn about how the extensions to 802.3 is used on aircraft, how that flight critical data is transferred in a timely matter, and how to manipulate the data on these networks. This progressive difficulty CTF provides a fun and informative way of approaching ARINC 664 networking.

SpeakerBio: Boeing
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: ARINC 664 CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

ARINC 664 is an extension to IP networking that adds deterministic QoS for Aircraft Systems over Ethernet. Sit down and learn about how the extensions to 802.3 is used on aircraft, how that flight critical data is transferred in a timely matter, and how to manipulate the data on these networks. This progressive difficulty CTF provides a fun and informative way of approaching ARINC 664 networking.

SpeakerBio: Boeing
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Friday - 11:00-12:59 PDT

Title: Arsenal: AI Goat
When: Friday, Aug 9, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 1 - Map

Description:

AI Goat is a deliberately vulnerable AI infrastructure designed to help security enthusiasts and pen-testers understand and exploit AI-specific vulnerabilities based on the OWASP AI Top 10. This arsenal session will demonstrate how to deploy AI Goat, explore various vulnerabilities, and guide participants in exploiting these weaknesses. Attendees will engage hands-on with the tool, gaining practical experience in AI security. Deployment scripts will be open-source and available after the session.

Speakers:Ofir Yakobi,Shir Sadon

SpeakerBio: Ofir Yakobi

Ofir Yakobi is a Security Researcher at Orca Security. With almost a decade of experience in detecting cybercriminals, malware research, and unveiling numerous security issues for high-profile companies, she brings her expertise in breaking and strengthening cloud vendors. She's as passionate at uncovering vulnerabilities as she is at picking her next travel destination.

SpeakerBio: Shir Sadon

Shir is a Cloud Security security and martial arts enthusiast! With a background in endpoints and servers cyber security, Shir once led research ventures to enhance departmental security. Now, Shir blends cybersecurity expertise with martial arts finesse, creating a formidable combination in the digital and physical realms

Return to Index - Add to Google - ics Calendar file

APV - Friday - 11:00-12:59 PDT

Title: Arsenal: CyberChef like Automation within BurpSuite - Let's get cooking with the CSTC
When: Friday, Aug 9, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 2 - Map

Description:

Imagine GCHQ's CyberChef integrated in BurpSuite with live modification of requests at your fingertips. That's exactly what we had in mind when we built the Cyber Security Transformation Chef (CSTC) a few years ago. The CSTC is an extension to the popular BurpSuite Proxy built for experts working with web applications. It enables users to define recipes that are applied to outgoing or incoming HTTP requests/ responses automatically. Whatever quirks and specialties an application might challenge you with during an assessment, the CSTC has you covered. Furthermore, it allows to quickly apply custom formatting to a chosen message, if a more detailed analysis is needed

Speakers: Matthias Göhring,Florian Haag

SpeakerBio: Matthias Göhring, Security Consultant and Penetration Tester at usd AG

Matthias Göhring is security consultant and penetration tester at usd AG, an information security company based in Germany with the mission #moresecurity. He is Head of usd HeroLab, the division of usd specialized in technical security assessments. In addition, he holds lectures at Technical University Darmstadt and University of Applied Sciences Darmstadt on ethical hacking and penetration testing. In previous scientific work, he focused on network and communication security as well as software security.

SpeakerBio: Florian Haag, Managing Security Consultant at usd AG

Florian Haag is a managing security consultant at usd AG with experience in penetration testing, software security assessments as well as code reviews. He is specialized in penetration tests of thick client applications, leveraging his background in software development to reverse engineer proprietary client applications and network protocols. In addition, he maintains several open source tools for web application pentesting presented at international conferences like BlackHat and DEF CON.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 13:00-13:59 PDT

Title: Arsenal: GraphQL Armor - Open Source GraphQL Security
When: Friday, Aug 9, 13:00 - 13:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 2 - Map

Description:

With our open-source tool GraphQL Armor we want to take GraphQL security to the next level. GraphQL Armor is a dead-simple yet highly customizable security middleware for various GraphQL server engines. It offers advanced protection against common vulnerabilities like query depth, complexity, and rate limiting.

In this session, we'll dive into the technical details, demonstrating how to identify GraphQL-specific vulnerabilities, integrate GraphQL Armor into your current setup, and customize it to your needs.

Speakers: Antoine Carossio,Tristan Kalos

SpeakerBio: Antoine Carossio

Former pentester for the French Intelligence Services. Former Machine Learning Research @ Apple.

SpeakerBio: Tristan Kalos

Tristan Kalos, co-founder and CEO at Escape, draws from a background as a software engineer and Machine Learning Researcher at UC Berkeley. Motivated by firsthand experience witnessing a client's database stolen through an API in 2018, he has since become an expert in API security, helping security engineers and developers worldwide building secure applications. He is an experienced keynote and conference speaker, presenting at Forum InCyber, bSides, APIdays, GraphQL conf, and other international software development and cyber security conferences.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 15:00-15:59 PDT

Title: Arsenal: HunterBounter - Swiss Army Knife for Bug Bounty
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 1 - Map

Description:

HunterBounter is an open-source tool designed to automate the scanning processes of tools like OpenVAS and ZAP Proxy using multiple Docker containers. Each container establishes a VPN connection to bypass security measures like IP bans during automated scans. The tool simplifies automated scanning for bug bounty hunters and penetration testers. Development is ongoing to integrate more open-source products for mobile, web application, and network scanning.

More information about the tool: https://hunterbounter.com Source code: https://github.com/hunterbounter

Demo Platform: https://panel.hunterbounter.com Username: AppSecVillage Password: gX8Q.Ja7!RMHD.kzSp!Zyu?AWGV

SpeakerBio: Utku Yildirim

Utku Yildirim is an experienced cybersecurity professional with a strong background in penetration testing and security evaluation. Currently working as a Senior Penetration Tester at Hoffmann Cybersecurity in the Netherlands. He also continues his role as a penetration tester at Cobalt.io. Utku has a diverse skill set encompassing network, web, API, and mobile application security testing.

His certifications include OSCE, OSCP, OSWP, and CRTO, among others. He has discovered multiple CVEs and has been recognized in international competitions such as NATO Locked Shields.

Utku is also a seasoned speaker, having presented at notable conferences like DEF CON 30 (Aerospace Village) , DEF CON 31(Telecom Village) and BSides Oslo, where he shared his insights on UAV security and SS7 hacking.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 15:00-15:59 PDT

Title: Arsenal: Introducing RAVEN - Discovering and Analyzing CI/CD Vulnerabilities in Scale
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 2 - Map

Description:

As the adoption of CI/CD practices continues to grow, securing these pipelines has become increasingly important. However, identifying vulnerabilities in CI/CD pipelines can be daunting, especially at scale. In this talk, we present our tooling, which we intend to release as open-source software to the public that helped us uncover hundreds of vulnerabilities in popular open-source projects' CI/CD pipelines.

RAVEN (Risk Analysis and Vulnerability Enumeration for CI/CD) is a powerful security tool designed to perform massive scans for GitHub Actions CI workflows and digest the discovered data into a Neo4j database. With RAVEN, we were able to identify and address potential security vulnerabilities in some of the most popular repositories hosted on GitHub, including FreeCodeCamp, Fluent UI by Microsoft, and much more. This tool provides a reliable and scalable solution for security analysis, enabling users to query the database and gain insights about their codebase's security posture

Speakers:
Elad Pticha,Oreen Livni

SpeakerBio:
Elad Pticha

Elad is a passionate security researcher with a focus on software supply chain and web application security. He dedicates his time to writing security research tools and finding vulnerabilities across a broad spectrum, from open-source projects and web applications to IoT devices and pretty much anything with an IP address.

SpeakerBio:
Oreen Livni

Oreen Livni is a passionate security researcher specializing in application and supply chain security, Domain, and networking. With a focus on software supply chain vulnerabilities. Alongside his professional commitments, he immerses himself in art, gardening, and the world of surfing, always seeking new experiences. With an unwavering commitment to staying updated on the latest security trends, he embraces new challenges and strives to make a difference in the cybersecurity landscape.

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 11:00-12:59 PDT

Title: Arsenal: Kubescape - OSS security from left to right and everything in the middle
When: Sunday, Aug 11, 11:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 1 - Map

Description:

As a security practitioner, you may find yourself tasked with securing cloud-native applications. The problem is that there are so many moving parts, that you just wish somebody would shine a light on the alerts that count, so you could focus. You also wish somebody could automate away the trial and error involved in getting the really complex things like network policies and seccomp profiles just right.

SpeakerBio: ben@armosec.io, CTO & Co-Founder at ARMO

Ben is a veteran cybersecurity and DevOps professional, as well as computer science lecturer. Today, he is the co-founder at ARMO, with a vision of making end-to-end Kubernetes security simple for everyone, and a core maintainer of the open source Kubescape project. He teaches advanced information security academically in both undergrad and graduate courses. In his previous capacities, he has been a security researcher and architect, pen-tester and lead developer at Cisco, NDS and Siemens.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 13:00-14:30 PDT

Title: Arsenal: SanicDNS
When: Saturday, Aug 10, 13:00 - 14:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 2 - Map

Description:

Most hackers have a love-hate relationship with DNS: teleporting a building block of the internet from the 80's is a recipe for frustration. To give DNS a modern twist, we developed an ultra-fast open-source DNS scanner, SanicDNS, which is two orders of magnitude faster than popular tools.

This Arsenal session will give a demonstration of how you can use SanicDNS to superpower your recon workflow using world's fastest DNS scanner.

SpeakerBio: Jasper Insinger

Jasper Insinger is a security researcher with a background in Electrical Engineering with a passion for low level / embedded computing. Before transitioning into security, Jasper worked on engineering the world's most efficient solar powered cars.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 11:00-11:59 PDT

Title: Arsenal: SCAGoat
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Arsenal 1 - Map

Description:

SCAGoat is a deliberately written vulnerable application designed for performing and learning Software Composition Analysis (SCA). There are many vulnerable web applications available to learn web app pentesting however there are not much resources to learn SCA, essentially applications built on vulnerable Open Source Software(OSS)

Speakers:Gaurav Joshi,HK,kvprashant

SpeakerBio: Gaurav Joshi

I am working extensively with Static Application Security Testing (SAST) as a security professional. My role involved conducting secure code reviews and utilizing SAST techniques to identify and mitigate vulnerabilities in software applications. As well as actively contribute to network focus on safeguarding potential threats.

SpeakerBio: HK

As a Product Security Engineer, my passion for cybersecurity drives me to excel in various areas. I specialize in conducting penetration testing, actively participate in security Capture The Flag (CTF) competitions, and perform code reviews to ensure secure code development. My expertise extends to leveraging Static Application Security Testing (SAST) techniques in languages like Java, Python, JavaScript, JSP, among others.

SpeakerBio: kvprashant

Prashant Venkatesh is an information security expert with over 20 years of experience. He presently works as Manager, Product security at Poshmark Inc,

Prashant is an enthusiastic participant in the field who consistently coordinates, reviews papers, and presents his work at numerous InfoSec conferences, including at Nullcon and c0c0n. He is also active through the OWASP Bay Area chapter Leadership and he is co-founder of annual Seasides Conference.

Gaurav Joshi is currently employed as a Product Security Engineer. His passion for cybersecurity propels him to excel in various areas. He specializes in conducting penetration testing, actively participates in security Capture The Flag (CTF) competitions, and performs code reviews to ensure secure code development. His expertise extends to leveraging Static Application Security Testing (SAST) techniques in languages like Java, Python, JavaScript, JSP, among others.

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 12:00-12:59 PDT

Title: Ask Me Anything - Daniel Cutberth, Moderated by Sudhanshu
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This is an AMA/Podcast that will be recorded on-site.

Speakers: Sudhanshu,Daniel Cuthbert

SpeakerBio: Sudhanshu
No BIO available
SpeakerBio: Daniel Cuthbert
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 17:30-21:30 PDT

Title: Ask the EFF
When: Friday, Aug 9, 17:30 - 21:30 PDT
Where: LVCC West/Floor 3/W307-W308 - Map

Description:

Electronic Frontier Foundation (EFF) is excited to be back at DEF CON. Our expert panelists will offer brief updates on EFF's work defending your digital rights, before opening the floor for attendees to ask their questions. This dynamic conversation centers challenges DEF CON attendees actually face, and is an opportunity to connect on common causes.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 11:30-11:59 PDT

Title: Atomic Honeypot: A MySQL Honeypot That Drops Shells
When: Friday, Aug 9, 11:30 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

Meet an attacking MySQL honepot which can “Attack the attackers”. In 2023 we have found a CVE (CVE-2023-21980) in MySQL that allows a rogue MySQL “server” to attack a client connecting to it; attack meaning RCE on the client side. Since then we were thinking on how to use it for good. One obvious application is to create a honeypot which will attack the attackers. In 2024 we have found another RCE in mysqldump utility (CVE-2024-21096), so we have created a rogue MySQL server and weaponized it with a chain of 3 vulnerabilities: 1/ arbitrary file read 2/ RCE from 2023 (CVE-2023- 21980) 3/ the new RCE (CVE-2024-21096). With this atomic honeypot we were able to discover 2 new attacks against MySQL server. Using arbitrary file read vulnerability in MySQL we were able to download and analyze the attackers' code and then execute an “attack against attackers” using a chain of exploits.

CVE-2023-21980 CVE-2024-21096

Speakers: Alexander Rubin,Martin Rakhmanov

SpeakerBio: Alexander Rubin, Principal Security Engineer, leading RDS Red Team at Amazon Web Services (AWS)

Alexander is a Principal Security Engineer at Amazon Web Services (AWS), leading RDS Red Team. Alexander was working as MySQL principal consultant/architect for over 15 years, started with MySQL AB in 2006 (company behind MySQL database), Sun Microsystems, Oracle and then Percona. His security pentest/red teaming interest started with playing CTFs and performing opensource security research. Alexander is managing RDS (relational database as a service) Red Team at Amazon Web Services.

SpeakerBio: Martin Rakhmanov, Senior Security Engineer, RDS Red Team at Amazon Web Services (AWS)

Martin is a Senior Security Engineer at Amazon Web Services (AWS) RDS Red Team. Prior to that, Martin spent 17 years doing security research of databases and other targets, including servers, desktop applications and hardware. Martin found more than 30 CVEs across various databases and other products.

Return to Index - Add to Google - ics Calendar file

Title: Attack and Defence in OT - Simulating attacks against hydroelectric power plants leveraging ICS Firing Ranges
When: Friday, Aug 9, 10:30 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

In this talk we will present the ICS firing range we built and hacked to simulate an actual attack against a hydroelectric power plant and create a DFIR training from the evidence left behind. The talk aims to emphasize the importance of attack simulation in the context of critical infrastructure and the potential benefit that firing ranges can provide to such assessments.

First we will examine the motivation behind the construction and usage of a firing range, covering various aspects including: - the threats operators of critical infrastructure face, - how security assessments are conducted in an OT context and - how an ICS firing range can be utilized to support them.

Next we will discuss the intended use cases of the firing range and the scenario it was made to display, the flooding of a hydroelectric power plant. As a result, the relevant components and production processes of the plant will be outlined. Then we will present and go into detail about the design & architecture of the firing range: - individual physical and virtual networks and components, - separate Active Directory environments, - implemented security measures - specific vulnerabilities intentionally left behind.

Picking up this last bullet-point, we continue with how we hacked the firing range and performed a Red Team assessment against it, simulating an actual attack. Starting with the C2 infrastructure we set up for the attack, we will guide the audience through the kill chain in chronological order and highlight the most important and relevant steps of the attack.

Once the offensive part of the talk concludes, a shift of perspective takes place and the attack is evaluated from the defence's point-of-view: we'll show how we identified, secured and analyzed indicators of compromise left behind by the attack. This includes the analysis of network captures, Windows event logs, memory dumps and more.

This talk will be presented by not only people from NVISO as the IT security service provider who built the firing range and performed to attack against it, but also by people from VERBUND's IT security team who actively use the firing range for training. This way we can involve both the attacker's and the defence's point-of-view.

Speakers: Julia Dewitz-Würzelberger,Bernhard Sedlmayer,Sarah Mader

SpeakerBio: Julia Dewitz-Würzelberger, Project Manager, OT Cyber Security at VERBUND

Julia Dewitz-Würzelberger is a project manager in the area of OT cyber security at VERBUND, Austria's largest energy supplier. Since 2023, she has been Head of the OT Cyber Security Lab, where she designs and implements concepts for innovative OT projects.

Her projects cover a broad spectrum, ranging from creating deception technology systems and the emulation of OT components to the operation of a quantum cryptography test setup.

As she can be interested in almost anything, she also completed a degree in anthropology and educational science before moving into IT/OT security.

SpeakerBio: Bernhard Sedlmayer

Bernhard Sedlmayer is a Security Engineer and Lego enthusiast. He is responsible for the OT security of the ICS/SCADA Systems at Austria's largest electricity provider with around 130 hydropower plants. He has 20 years of experience in the energy supply industry and supports many innovative and fundamental projects in operational technology as an OT security

specialist. Red Teaming and pentesting on Windows and Linux Systems is also one part of his daily to-do's.

SpeakerBio: Sarah Mader, Senior Consultant at NVISO

Sarah is a Senior Consultant at NVISO, with a focus on Red Team Assessments. Complementing her cybersecurity experience, she has developed proficiency in Operational Technology (OT) assessments and continues to specialize further in this area.

She possesses a Master's degree in Applied IT Security, which has been enriched by her diverse experiences in cybersecurity roles across various companies.

In addition to her professional work, Sarah is dedicated to contributing to the community by leading workshops and delivering presentations at industry conferences.

Return to Index - Add to Google - ics Calendar file

Title: Attack Vectors of Quantum Computers
When: Friday, Aug 9, 16:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

This talk explores security issues in quantum computing, identifying attack vectors on major platforms like IBM and IonQ. We examine vulnerabilities in popular quantum software development kits (SDKs) and workflows, highlighting flaws in authentication token management and supply chain attacks that inject malicious circuits.

We also review existing literature on vulnerabilities in Quantum Processing Units (QPUs) and present new attacks that exploit qubit reset quality to infer results from prior computations and tamper with subsequent ones. Additionally, we demonstrate how crosstalk can inject faults into circuits run by other tenants on the same QPU.

Quantum computing holds immense potential, but so does the responsibility to secure it. By understanding and addressing these vulnerabilities today, we can build a more secure quantum ecosystem.

Speakers: Sorin Boloș,Adrian Coleșa

SpeakerBio: Sorin Boloș

Sorin Boloș is a software engineer turned to quantum computing. After earning his stripes in the tech world and diving deep into computer science, he had a fling with quantum computing, thanks to a flirty course by MIT, and it turned into a full-blown love affair. As a proud Qiskit Advocate, he has been spreading the quantum love through talks, courses, and hosting some cool minds. Now, he is on a mission to crack the code on quantum security.

SpeakerBio: Adrian Coleșa

Adrian Coleșa is an Associate Professor of Computer Science at the Technical University of Cluj-Napoca (TUCN) in Romania, where he has dedicated 26 years of service. He earned his PhD from TUCN and specializes in teaching courses such as Operating Systems (OS), Secure Coding, and Virtualization-Based Security. His primary research focus since 2013 has been in the field of cybersecurity. Additionally, he has been leading a cybersecurity master's program at TUCN since 2015. Since 2019, he has held the position of Senior Security Researcher at Bitdefender, concentrating on virtualization and operating system security. Adrian obtained the OSCP certification in 2014. He has coauthored around 40 scientific papers and six US patents, primarily in cybersecurity.

Return to Index - Add to Google - ics Calendar file

PYV - Friday - 13:00-13:59 PDT

Title: Attacking and defending card present transactions
When: Friday, Aug 9, 13:00 - 13:59 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

In this workshop we present two perspectives on card present attacks - attacker's and defender's. What typical banks and card processors think of modern card present attacks? How easy is it to mitigate those without compromising on user experience?

Speakers: Yurii Zadoianchuk,Stephan Viljoen,Sebastiaan Pierrot

SpeakerBio: Yurii Zadoianchuk, Adyen
No BIO available
SpeakerBio: Stephan Viljoen, Adyen
No BIO available
SpeakerBio: Sebastiaan Pierrot, Adyen
No BIO available

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 14:30-15:10 PDT

Title: Attacking and Defending Software Supply Chains: How we got Admin in your Clouds!
When: Friday, Aug 9, 14:30 - 15:10 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

This talk will explore how default configurations in reference architectures of our most commonly used software supply chain services can lead to a handful of unsavory outcomes including secrets exfiltration, lateral movement, and privilege escalation within production cloud and SaaS environments. We'll take a close look at how many of the interactions between people and CI|CD services are not as safe as we think. Some examples we'll look at:

```
- Abusing PRs against Github repositories allows for execution of code prior to code review & merge,
- Multi-tenant infrastructures in CI like Buildkite lead to over-authorization & access to productio
- Lacking Pipeline Based Access Control (PBAC) in CI services like Buildkite leads to code execution
```

After we identify the pitfalls in our by-default configurations, we'll demonstrate how best to modify them using available tools, services, & best practices.

SpeakerBio: Mike Ruth

Mike is a Senior Staff Security Engineer at Rippling, where he works on securing the world's best All-In-One HR & IT Platform. Previously the technical lead for Infrastructure Security at companies such as Brex & Cruise, Mike has over thirteen years of experience securing, designing, and deploying cloud infrastructure & SaaS services.

Return to Index - Add to Google - ics Calendar file

CPV - Saturday - 17:00-17:30 PDT

Title: Attacks on GenAI data and using vector encryption to stop them
When: Saturday, Aug 10, 17:00 - 17:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

As the adoption of GenAI tools has soared, security has done little to keep up. New classes of data, and especially vector data, is flooding into new and untested data stores. Vector databases are getting copies of health data, financial data, HR data, emails, and everything else, but they have no intrinsic security. What's worse, the vectors themselves can be reversed in embedding inversion attacks that turn those vectors back into faces, sentences, and even pictures. We discuss these new attacks and a new branch of cryptography, vector encryption, which allows for privacy preserving searches to happen over the encrypted vectors. We'll discuss the benefits, trade-offs, and current state of the field and the open source software we've built to meet the new need.

Speakers: Bob Wall,Patrick Walsh

SpeakerBio: Bob Wall
No BIO available
SpeakerBio: Patrick Walsh, IronCore Labs

Patrick Walsh has more than 20 years of experience building security products and enterprise SaaS solutions. Most recently he ran an Engineering division at Oracle, delivering features and business results to the world's largest companies. Patrick now leads IronCore Labs, a data privacy platform that helps businesses gain control of their data and meet increasingly stringent data protection needs.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 12:00-12:59 PDT

Title: Austin School For The Driven
When: Saturday, Aug 10, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Return to Index - Add to Google - ics Calendar file

DL - Friday - 14:00-15:45 PDT

Title: Automated Control Validation with Tommyknocker
When: Friday, Aug 9, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W303 - Map

Description:

Tommyknocker is an open source project designed to facilitate automation of continuous security control validation, bringing some of the processes developers have been using for years for regressing testing, to the security world. It allows users to easily create test scenarios using docker images and standard scripts to perform one or more test actions, followed by the ability to easily check common tooling (SIEM, IDS, Log aggregators) for any expected alerts or log entries. Using Tommyknocker, security organizations can add test cases each time a new security control is created, so that any time a change is made in the environment, the continued functioning of existing controls can be validated. Many times, security organizations will only test controls when they are first implemented, and potentially a few times a year for audit purposes. With Tommyknocker, controls can be tested multiple times per day, ensuring that alerts are raised as soon as possible when a control ceases to function correctly, or is compromised by a threat actor.

SpeakerBio: Jeremy Banker

Jeremy is an accomplished software developer and lifelong hacker with a combined 10 years of experience in software development and cybersecurity. After working his way up from customer support, and earning a Master's degree in Information Security, Jeremy helped found the Security Product Engineering, Automation and Research group at VMware. Having spoken at both Blackhat Arsenal and Def Con Demolabs on his open source projects, he continues to be passionate about sharing new tools and technologies with the community. In his spare time, Jeremy enjoys gardening, camping, and tinkering with all manner of technology.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 12:00-12:45 PDT

Title: automobiles, alcohol, blood, sweat, and creative reversing of an obfuscated Car-Modding tool
When: Saturday, Aug 10, 12:00 - 12:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

reversing can feel uber powerful... like you hold God's honest truth within your hands... most humans don't understand what you can see and comprehend.

until someone tries to hide the truth from you... limit your knowledge... keep you from your glorious purpose!

obfuscated code can be a real downer.

this talk focuses on the story of how i took on an interesting obfuscated target (an automotive modder's tool with ability to flash firmware and tweak engines), in fun and exciting ways.

we'll discuss several problems with obfuscated code, an approach i took (and tooling), playing in the guts of machine code, and customizations to binary analysis tools that came out of the journey...

there will be much hex, disassembly, green on black, total carnage.

you will walk away with powerful ideas and new tools to help you in your pursuit of truth. you will be entertained, enriched, educated, and hopefully inspired. instead of thinking that "atlas is smart" my goal is you feeling, and being, more powerful.

come with Vivisect installed to follow along!

- link
- link
- link
- link

SpeakerBio: atlas

atlas is a doer of things. with nearly 20 years of experience binary reverse-engineering, exploiting, and bringing friends along, he's as likely to talk about RF signals as to discuss converting machine language bits into assembly instructions, intermediate languages, and decompilers. driven by the "truth", and desire to write tools to make finding truth easier, his talks always engage, embrace, and baffle.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 11:30-11:59 PDT

Title: Aviation cybersecurity lightning talk: Three topics in thirty minutes
When: Friday, Aug 9, 11:30 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

This is going to be a lightning talk covering three short aviation cybersecurity topics. 1) What is the attack surface of an airport 2) How plane hacking is represented in the movies 3) What it takes to resolve a 3 year disclosure process for an EFB.

SpeakerBio: Ken Munro, Partner and Founder at Pen Test Partners

Ken Munro is Partner and Founder of Pen Test Partners, a firm of ethical hackers. He and colleagues hold private pilot's licenses and have been interested in aviation security for many years. They also publish and blog about their research into aviation cyber security, covering topics from airborne connectivity, the potential risks of publicly available avionics component information, and even the entire attack surface of the modern airport. Ken and Pen Test Partners have also been invited to speak at various aviation industry events, and on aviation at specialist security events such as DEF CON's Aerospace Village, the Global Connected Aircraft Summit, and the Aviation ISAC Summit among others.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-12:59 PDT

Title: Aw, man…pages!
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

How well do *you* know your man pages? Find out by teaming up with up to 3 other people (or come solo and get matched up with some new friends) and play "Aw, man...pages!". Across several rounds, your knowledge of man pages will be tested to the limit. Can you remember what command line flag is being described by its help text? Can you identify a tool just from a man page snippet? Can you provide the long-form flag when only given the short? Will you prove yourself worthy to be crowned the man page champion?

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 10:00-10:45 PDT

Title: AWS CloudQuarry: Digging for secrets in public AMIs
When: Sunday, Aug 11, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

Join us as we unravel another story of public resources from AWS, digging in 3.1 million AMIs for secrets. Beyond the findings, we'll delve into the ominous connection between exfiltrated AWS access credentials from these AMIs and the heightened risk of AWS account takeover. This talk will highlight key methodologies, tools, and lessons learned, emphasizing the critical need for robust security measures in the cloud to prevent both data exposure and potential account compromise.

We started and developed this research without references of existing work. However, here are two links that can be viewed as related/previous work:

This article shows a research on a subset of public AMIs from a single region in AWS link

This research shows a similar issue where public EBS are scanned. However, this technique does not work for most public AMIs link

Speakers: Eduard Agavriloae,Matei Josephs

SpeakerBio: Eduard Agavriloae, AWS Offensive Expert and Pentester

Eduard focuses on cloud and offensive security. He’s an experienced penetration tester and in the last years he started doing novel research, writing articles, developing tools like EC2StepShell and presenting at security conferences.

SpeakerBio: Matei Josephs, Senior Penetration Tester

Matei is a Senior Penetration Tester who loves exploring the internet for vulnerabilities. Matei has discovered several CVEs and has the OSCP, CRTO, eWPT and a few other certifications alongside a Master's degree in Cybercrime and Intelligence. Although his daily job requires him to conduct thorough tests across a limited scope, after work, Matei enjoys doing simple tests across the whole internet.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 13:00-14:50 PDT

Title: Badge Cloning: A Penetration Tester's Guide to Capturing and Writing Badges
When: Friday, Aug 9, 13:00 - 14:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

In this workshop, we distill key tactics from the comprehensive Practical Physical Exploitation course, tailored specifically for penetration testers looking to attack Physical Access Controls (PACS).

Participants will embark on a journey through the ins and outs of cloning badges during physical penetration tests. Explore the intricacies of long-range, short-range, and Stealth cloning tactics, gaining hands-on experience in the art of badge duplication. Delve into the realm of implantable devices, understanding their role in modern access control exploitation.

Join us as we uncover the nuances of downgrade/upgrade attacks and the protocols that make them possible. Learn to navigate the landscape of access control systems with expert guidance, equipping yourself with the knowledge to identify and exploit vulnerabilities.

By the end of this session, you'll wield an arsenal of cutting-edge techniques, ready to transform your facility into a bastion of high-security readiness. Don't miss this opportunity to elevate your skills and refine your physical security penetration testing skills.

Speakers: Travis Weathers,Ralph May

SpeakerBio: Travis Weathers
No BIO available
SpeakerBio: Ralph May, Security Analyst and Penetration Tester at Black Hills Information Security (BHIS)

Ralph is a security analyst and penetration tester at Black Hills Information Security. Ralph is also a co-developer and instructor of the Practical Physical Exploitation course. Before joining BHIS, Ralph spent five years performing offensive operations on a wide range of security assessments. These assessments include physical, wireless, network, social engineering, and full simulation red teams. Before focusing on security, Ralph worked as a system administrator and network engineer for civilian and government employers. Ralph is a US Army veteran who previously worked with the United States Special Operations Command (USSOCOM) on information security challenges and threat actor simulations.

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 15:00-15:30 PDT

Title: Basic Mobile Phone Privacy
When: Friday, Aug 9, 15:00 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Curious about mobile phone privacy? Come on over for this workshop with lots of direct Q&A!

SpeakerBio: Grey Fox

Grey Fox, the callsign assigned to him by a DHS colleague, recently retired from the U.S. military after 20 years of service as an intelligence analyst, language analyst, digital network intelligence targeter, cyberspace mission leader, and digital defense education program leader. Having deployed eight times supporting front line combat teams, his experience ranges from offensive cyberspace operations planning and execution to military information support operations. Along the way, Grey Fox acquired multiple creds, including GCTI, GASF, GAWN, and CWNA. He currently instructs Digital OPSEC at the U.S. Army Security Cooperation Officer course and the U.S. Air Force Research Lab, as well as SDR foundations and Wi-Fi hacking at the U.S. Army Signal School.

Return to Index - Add to Google - ics Calendar file

CPV - Saturday - 12:30-12:59 PDT

Title: Basic Mobile Phone Privacy
When: Saturday, Aug 10, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Curious about mobile phone privacy? Come on over for this workshop with lots of direct Q&A!

SpeakerBio: Grey Fox

Grey Fox, the callsign assigned to him by a DHS colleague, recently retired from the U.S. military after 20 years of service as an intelligence analyst, language analyst, digital network intelligence targeter, cyberspace mission leader, and digital defense education program leader. Having deployed eight times supporting front line combat teams, his experience ranges from offensive cyberspace operations planning and execution to military information support operations. Along the way, Grey Fox acquired multiple creds, including GCTI, GASF, GAWN, and CWNA. He currently instructs Digital OPSEC at the U.S. Army Security Cooperation Officer course and the U.S. Air Force Research Lab, as well as SDR foundations and Wi-Fi hacking at the U.S. Army Signal School.

Return to Index - Add to Google - ics Calendar file

HRV - Sunday - 11:00-11:30 PDT

Title: Basic Packet Radio Operation
When: Sunday, Aug 11, 11:00 - 11:30 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

Do you ever pine for the days of 1200bps communications? Learn how to leverage the power of amateur radio to send digital data, pictures, and even cat memes using packet radio. This presentation will crack open the basics of packet, explore the tools you need (no soldering iron required!), and show you how to join the network buzzing beneath the surface of the RF spectrum.

SpeakerBio: Jeremy
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Bastardo Grande: Hunting the Largest Black Market Bike Fence In The World
When: Friday, Aug 9, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Since 2020, I have (as a BikeIndex.org cofounder) been chasing and hunting the single largest black market bike fence in modern history. This OSINT-heavy, cross-border investigation eventually blossomed into a federal court case in early 2024, so I've only able to partially share that story in public until now. By the time DEFCON happens, I'll be able to give this talk in its fullest and most unredacted form, which I haven't been able to do yet. (This talk was presented at Seattle BSIDES 2023, but even then I couldn't give 'the whole talk' because one of the key players was still being prosecuted in CA court)

In December 2021, BikeIndex.org published an article that laid out how our OSINT detective work showed residential burglars in Colorado were exporting stolen bikes to Juarez Mexico and selling them on grey-market sites there for excellent profit. This quantified a long suspected 'urban legend' in the cycling community - that high end stolen bikes went to Mexico - but also the economics of the problem, as we tracked over 1000 sales of stolen bikes and were able to capture sales data and study the black market in very great detail. (That write up is here, if you are curious:https://bikeindex.org/news/closing-the-loop-a-deep-dive-on-a-facebook-reseller-of-bikes-stolen-in)

What we did *not* disclose at that time was that we were infiltrating and tracking an even larger, more impressive criminal actor in the same space - one whose sales and profits reach into the millions. Through years of surveillance, OSINT work, and a lot of persistence, we eventually identified one of his US side suppliers and got them raided by law enforcement, which then snowballed into a federal prosecution in 2024.

In this talk, I'll talk about how the motivation to seek justice drives normal people to do extraordinary things with OSINT and other crafty methods to chase down bad guys and recover their stolen goods and seek justice. I'll cover some of the crazier edge cases we've run into in this space, and I'll talk about the secret shadow army of hunters and cyclists who are hunt these kinds of bad guys down online, every day.

The talk will be audience engaging, with back-and-forth and audience 'spot-the-OSINT-FAIL-here' type participation as we walk through the major breakthroughs that took this project from 'hey, that's an interesting' to names going down into a federal indictment. Specifically, I'll give an overview of how we engage with theft victims to surveil, track, identify, and take down transnational black market bike fences - who often turn out to be even crazier individuals than anybody ever expected.

SpeakerBio: Bryan Hance
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-10:59 PDT

Title: Be Latino in Cybersecurity on markets outside LATAM
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

En este panel se abordará las oportunidades y desafíos que enfrentan los profesionales latinos en el campo de la ciberseguridad fuera de América Latina. Adicionalmente estudiaremos las estrategias para destacar en mercados internacionales, las habilidades clave necesarias y las redes de apoyo que pueden ayudar a los latinos a prosperar en esta industria en constante evolución. Además, se discutirán experiencias personales y consejos prácticos para navegar en entornos multiculturales y globales. Únete a nosotros para aprender cómo los latinos pueden hacer una diferencia significativa en el panorama global de la ciberseguridad.

Speakers: Salvador Mendonza,Lenin Alevski,Omar Santos,Alan Villaseñor,Guillermo Buendia

SpeakerBio: Salvador Mendonza
No BIO available
SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog

SpeakerBio: Omar Santos
No BIO available
SpeakerBio: Alan Villaseñor
No BIO available
SpeakerBio: Guillermo Buendia
No BIO available

Return to Index - Add to Google - ics Calendar file

XRV - Friday - 17:00-17:59 PDT

Title: Be the Ghost in the Shell Barrier Mazes FTW
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Using AI to pre-generate gamifie CTFs so hard even the admins won't know the answers. Exploring the visionary concept of using gamified, AI-generated barrier mazes for futuristic authentication and encryption inspired by manga. But in the great words of your Mom and mine, if we aren't breaking into something, then what is David Maynor even doing there?

SpeakerBio: David "Icer" Maynor, Secret Keeper at ThreatHunter.ai

David “Icer” Maynor, Secret Keeper at ThreatHunter.ai, has over 20 years of experience in information security with deep technical expertise in threat intelligence, reverse engineering, exploit development, and offensive security testing. Results-driven research, analysis, and solutions leveraging partnerships and cross-disciplinary teams, to strengthen customer and business security posture and capabilities. Served as founder, executive, and advisor within the information security startup space. Author of and contributor to several popular open-source tools, presenter and instructor, and subject matter expert contributor for print, television, and online media.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 13:30-14:15 PDT

Title: Behind Enemy Lines: Engaging and Disrupting Ransomware Web Panels
When: Saturday, Aug 10, 13:30 - 14:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Ransomware groups have become notably proficient at wreaking havoc across various sectors , but we can turn the tables. However, a less explored avenue in the fight against these digital adversaries lies in the proactive offense against their web panels. In this presentation, I will delve into the strategies and methodologies for infiltrating and commandeering the web panels used by ransomware groups to manage their malicious operations or the APIs used during their initial exfiltration of data.

I will demonstrate how to leverage these vulnerabilities to gain unauthorized access to the ransomware groups' web panels. This access not only disrupts their operations but also opens a window to gather intelligence and potentially identify the operators behind those APTs. Let’s explore the frontiers of cyber offense, targeting the very command and control (C2) centers ransomware groups rely on, turning the tables in our ongoing battle against cyber threats,it’s our turn to wreak havoc.

- link
- link
- link
- link
- link
- link

SpeakerBio: Vangelis Stykas, Chief Technology Officer at Atropos

Vangelis began as a developer from Greece. Six years ago he realized that only his dog didn’t have an API, so he decided to steer his focus towards security.

That led him to pursue a PhD in Web Application Security with an extra focus on machine learning. He’s still actively pursuing it.

He currently applies his skills as a Chief Technology Officer at Atropos, and during his free time, Vangelis is helping start-ups secure themselves on the internet and get a leg up in security terms.

His love of a simplistic approach to hacking by exploiting vulnerable APIs led him to publish research regarding API controlling ships, smart locks, IP cameras, car alarms, EV chargers, and many other IoT devices. Since our lives are nowadays extremely cyber-dependent, his goal is to convince all companies to never neglect their API security as rush-to-market mentality is almost certain to lead to catastrophic security failure.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 10:00-10:45 PDT

Title: Behind Enemy Lines: Going undercover to breach the LockBit Ransomware Operation
When: Friday, Aug 9, 10:00 - 10:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

Delve into the clandestine world of the LockBit ransomware gang! In this revealing presentation, I will recount my two-year journey spent infiltrating the inner ranks of the LockBit crime syndicate. Learn about the strategies employed to earn the trust of key individuals within the syndicate, including the gang's leader, LockBitSupp.

You will see firsthand accounts of these exchanges, and I will detail the intricacies of my relationship with LockBit's leadership and its network of affiliate hackers. You will also gain insight into the unintended consequences of my actions, including how my perceived breach of their infrastructure impacted the syndicate's operations. More importantly, I will share how I assisted in unmasking the real-world person behind the mask of LockBitSupp.

Join me as I illustrate the pivotal role of human intelligence in tandem with cyber threat intelligence to combat ransomware threats. This talk offers a compelling narrative of real-world efforts to thwart ransomware activities and safeguard organizations from LockBit ransomware attacks.

- 60 min (full episode): 4/14/2024: Scattered Spider; Knife; Tasmanian Tiger - CBS News
- 60 Min Overtime (additional footage from my interview about LockBit): Infiltrating ransomware gangs on the dark web - CBS News
- Ransomware Diaries
- Ransomware Diaries: Volume 1 | Analyst1
- Ransomware Diaries V. 2: A Ransomware Hacker Origin Story (analyst1.com)
- Ransomware Diaries V. 3: LockBit's Secrets (analyst1.com)
- Ransomware Diaries Volume 5: Unmasking LockBit (analyst1.com)

SpeakerBio: Jon DiMaggio, Chief Security Strategist at Analyst1

Jon DiMaggio is the chief security strategist at Analyst1 and has over 16 years of experience hunting, researching, and writing about advanced cyber threats. In 2022, Jon's authored his first book, "The Art of Cyberwarfare," which earned him the prestigious SANS Difference Makers Award, solidifying his status as a thought leader in the industry. The following year, SANs recognized his work once again, awarding his most notable research, "The Ransomware Diaries," detailing his operation to infiltrate the real-world humans behind the LockBit criminal operation. Jon’s other notable achievements include his appearance on 60 Minutes, where he discussed his undercover operations infiltrating some of the world top ransomware gangs. Jon’s research has been featured in The New York Times, Wired, Bloomberg, Fox, CNN, Reuters, and other news organizations.

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 12:30-12:59 PDT

Title: Behind the Badge: How we used and abused hardware to create the AV badge for DC32
When: Sunday, Aug 11, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

ADS-B aircraft tracking has long been done with Raspberry Pi's and SDRs. We set out to build our own receiver from the ground up, but without resorting to expensive and power-hungry SDR chips. Join us for a behind-the-scenes look as we walk through how we were able to (ab)use hardware to squeeze an entire Linux system, custom signal processing chain, and map visualizer into a chip that costs less than most microcontrollers.

Speakers: Adam Batori,Robert Pafford

SpeakerBio: Adam Batori
No BIO available

SpeakerBio: Robert Pafford

Robert Pafford graduated summa cum laude from The Ohio State University with a B.S. in Electrical and Computer Engineering this past May. During his time there, he was an avid participant in Ohio State's Underwater Robotics Team, leading the team to top placement in an international autonomous underwater vehicle competition where he led the design of the vehicle's next generation electronics system. Robert's passion for problem-solving and cutting-edge technology led him into reverse engineering, where, starting this fall, he will work as an Associate Engineer at STR, a national-security focused technology firm.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 16:00-16:50 PDT

Title: Bespoke C2s are coming of age.
When: Saturday, Aug 10, 16:00 - 16:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

This talk introduces a method for creating unique command and control (C2) servers for each engagement, utilizing diverse programming languages, obfuscations, and communication protocols. The approach leverages a curated repository of historical C2 and implant data, with feedback to ensure continuous improvement. Want a C2 written in PERL that uses Gopher for comms? I don't know why you would but I can show you how. Rust, nodejs, and more. Want a C2 that runs in UEFI? The best part is once the engagement is done you don't have to worry that your toolset was blown because next engagement you will have a new framework.

SpeakerBio: David "Icer" Maynor, Secret Keeper at ThreatHunter.ai

David “Icer” Maynor, Secret Keeper at ThreatHunter.ai, has over 20 years of experience in information security with deep technical expertise in threat intelligence, reverse engineering, exploit development, and offensive security testing. Results-driven research, analysis, and solutions leveraging partnerships and cross-disciplinary teams, to strengthen customer and business security posture and capabilities. Served as founder, executive, and advisor within the information security startup space. Author of and contributor to several popular open-source tools, presenter and instructor, and subject matter expert contributor for print, television, and online media.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 11:00-11:59 PDT

Title: Betting on Your Digital Rights: 3rd Annual EFF Benefit Poker Tournament at DEF CON 32
When: Friday, Aug 9, 11:00 - 11:59 PDT
Where: Other / See Description

Description:

Begins Friday at 12: 00 (11:00 for the pre-tournament poker clinic)

We’re going all in on internet freedom. Take a break from hacking the Gibson to face off with your competition at the tables—and benefit EFF! Your buy-in is paired with a donation to support EFF’s mission to protect online privacy and free expression for all. Play for glory. Play for money. Play for the future of the web. Seating is limited, so reserve your spot today.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 12:00-17:59 PDT

Title: Beverage Chilling Contraption Contest
When: Saturday, Aug 10, 12:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-B - Map

Description:

The Beverage Chilling Contraption Contest has been un-canceled! After a fantastic afternoon of day drinking celebrating the start of the 20th BCCC we've run out of beer. It's a disaster, a catastrophe! Fortunately, we had the wherewithal to scramble a crack beverage acquisition team to the streets of Las Vegas and found more! Don't ask where. Unfortunately, like the streets of Las Vegas, it's HOT and kinda sticky. We need you to help us fix this and get that beer as cold as the barren wasteland that is our generation's dreams of home ownership!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-15:59 PDT

Title: Beverage Chilling Contraption Contest
When: Friday, Aug 9, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-B - Map

Description:

The Beverage Chilling Contraption Contest has been un-canceled! After a fantastic afternoon of day drinking celebrating the start of the 20th BCCC we've run out of beer. It's a disaster, a catastrophe! Fortunately, we had the wherewithal to scramble a crack beverage acquisition team to the streets of Las Vegas and found more! Don't ask where. Unfortunately, like the streets of Las Vegas, it's HOT and kinda sticky. We need you to help us fix this and get that beer as cold as the barren wasteland that is our generation's dreams of home ownership!

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 17:00-17:30 PDT

Title: Beyond Sunset: Exposing the Occultations Lurking in Large-Scale Off-Grid Solar Systems
When: Friday, Aug 9, 17:00 - 17:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

This talk reveals stunning vulnerability findings in leading solar manufacturers that, when exploited, the stake is the grid. We'll explore three massive vulns in the management platform and discuss how they can be weaponized to become chilling nation security risks.

Speakers: Alexandru Lazar,Dan Berte

SpeakerBio: Alexandru Lazar, Security Researcher at Bitdefender

Alexandru Lazar is a Security Researcher at Bitdefender. He has red team and penetration testing experience and specializes in IoT and embedded systems with a focus on reverse engineering vulnerability assessment and exploitation. He has disclosed vulnerabilities to vendors such as Amazon Bosch LG with his research being covered by several media publications.

SpeakerBio: Dan Berte, Manager, IoT Vulnerability Research Program at Bitdefender

Dan manages the Bitdefender IoT vulnerability research program. He previously lead the design and product experience at Bitdefender. His team designed and built Bitdefender BOX, a revolutionary device that protects connected devices in smart homes.

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 09:00-09:30 PDT

Title: BIC United Kingdom Chapter Informational Virtual Opening Session
When: Friday, Aug 9, 09:00 - 09:30 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Meet BIC @ UK! The U.K. Chapter of Blacks In Cybersecurity is dedicated to empowering Black professionals in the United Kingdom. This session will introduce you to the regional leaders and their vision for their local chapter and members.

SpeakerBio: Ike Marizu, BIC U.K. Ambassador
No BIO available

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 10:00-10:59 PDT

Title: BIC Village Keynote: Cyber Threat Landscape And Law Enforcement
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Cybersecurity threats are increasingly sophisticated and pervasive. This talk provides a overview of the current threat landscape, highlighting key trends like ransomware, state-sponsored attacks, and supply chain threats. We will explore how law enforcement combats cybercrime through innovative investigation techniques, international collaboration and evolving legal frameworks. Gain actionable insights to strengthen your cybersecurity posture and understand the critical role of law enforcement in maintaining digital security.

SpeakerBio: Kevin Parker, Cybersecurity and Privacy Researcher at Blacksuit Consulting

Kevin Parker is the principal at Blacksuit Consulting and a retired FBI Special Agent. He served as the lead agent for state sponsored computer intrusion investigations and pursued foreign threat actors. Kevin investigated criminal computer intrusions, collected evidence and arrested numerous subjects while providing actionable intelligence to investigations across the FBI.

Kevin served several years as a liaison to private sector and the Defense Industrial Base (DIB) in the roles of FBI Infragard and Strategic Partnership Coordinator. In these roles he brought security awareness and security best practices to critical infrastructure organizations.

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 09:30-09:59 PDT

Title: BIC Village Opening Q&A with Marcus Hutchins
When: Friday, Aug 9, 09:30 - 09:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

In this Q&A session featuring a malware engineer, the BIC community will engage with insights and inquiries!

Speakers: Michaela Barnett,Marcus Hutchins

SpeakerBio: Michaela Barnett, Red Team Operator & Cybersecurity Researcher

Michaela is the founder of Blacks In Cybersecurity (BIC). She is a Penetration Tester and Researcher in the fields of BioCybersecurity & Maritime Cybersecurity. Michaela initially ventured into greater service of the Cybersecurity community through the founding and continued leadership of Blacks In Cybersecurity.

SpeakerBio: Marcus Hutchins, Cybersecurity Speaker

Marcus Hutchins is best known for stopping one of the largest cyberattacks in history, the 2017 WannaCry ransomware attack. At the age of 13, Marcus was given his first computer, enabling him to begin teaching himself programming. Throughout his teen years he alternated between different programming languages, learning VB, PHP, C, C++, and Assembly. Due to almost exclusively hanging around hacking communities, he eventually found himself making money writing and selling illegal hacking tools. In 2013 Marcus started MalwareTech, an anonymous blog focused on detailing the deep and technical inner workings of malware. The blog became popular among both security professionals and criminal hackers alike. As time went on, he became increasingly uncomfortable with working for cybercriminals and focused on leaving that life behind. Through his blog, Marcus had received several high paying job offers from international security companies, and gained some understanding of the cybersecurity industry. In 2016, he made the decision to transition into cybersecurity, taking a job as a research and development lead at a Los Angeles based firm. On May 2017, Marcus gained worldwide media attention after being outed as the person who stopped WannaCry, an extremely destructive ransomware virus. Reporters were able to track his MalwareTech alias back to his real identity, thrusting him into the spotlight. Three months later, he was arrested by the FBI while attending DEF CON, the world's largest hacking convention.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Biohacking Village CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map

Description:

A scenario-driven Capture the Flag contest, pits teams of participants against adversaries and a clock, to protect human life and public safety. Participants compete against each other on both real and simulated medical devices, integrated into the fully immersive Biohacking Village: Device Lab, laid out as a working hospital.

Challenges will be tailored for all skill levels and draw from expertise areas including forensics, RF hacking, network exploitation techniques, web security, protocol reverse engineering, hardware hacking, and others. You will hack actual medical devices and play with protocols like DICOM, HL7 and FHIR.

2024 Capture the Flag Challenge

Welcome, elite hackers and cyber sleuths, to a CTF experience like no other - the "Code D.A.R.K. : Biohacking Village CTF Challenge".

Merge the worlds of biology and cybersecurity in an adrenaline-pumping contest that tests your skills in ways you've never imagined. Thrilling and challenging cybersecurity adventure centered around a hospital setting as a scenario where participants engage in a race against time to secure or retrieve critical medical data, navigating through various cybersecurity puzzles and challenges, where participants act as guardians of critical biological data.

Unravel Biological Mysteries: Dive into a narrative where biotechnology meets cyber-warfare. Decode genetic puzzles, breach virtual lab networks, and outsmart bioinformatics security systems.

Elevate Your Hacking Game: Challenge yourself with unique biocybersecurity scenarios. This isn't your typical CTF - it's a fusion of biotech intrigue and hardcore hacking.

Compete and Collaborate: Team up with fellow biohackers and cyber warriors. Share knowledge, strategize, and show off your skills in a community where biology and bits intersect.

Gear Up for a Cyber-Biotech Showdown

Immersive Scenarios: Each challenge is a step into a world where safeguarding biological data is as critical as securing digital assets.

Skill Diversity: Whether you're a veteran hacker or a biotech enthusiast, Code D.A.R.K. offers a range of puzzles that cater to a wide array of skills and interests.

- OT/IT
- Medical devices
- Hospital infrastructure
- Regulatory and international affairs
- Robotics
- Data
- **Mark your calendars** and set your alarms because the action kicks off on Friday, August 9th at 1000 PDT.
- **Play from anywhere in the world!** CTF open hours are as follows:
    - ♦ Friday, August 9th from 10am PST - 6pm PDT
    - ♦ Saturday, August 10th from 10am PST - 6pm PDT

♦ Sunday, August 11th from 10am PST - 12pm PDT

RULES

REGISTRATION

Participants may only register once for this challenge. If participants register for this challenge more than once, the whole teams with a participant that registered multiple times will be disqualified.

By registering, participants agree that their accounts may be rejected or terminated and all submissions by them and/or their Team may be disqualified if any of the information in their account is incorrect.

Participants must agree to and abide by the Code of Conduct while participating in the Biohacking Village Capture the Flag. Anyone who will conduct themselves against the CoC will be eliminated from competition and banned forever.

TEAMS

After participants register individually, they may work alone (team of one) or on one team with other challenge participants. To work on a team, they may either create a new team or join one that is pre-existing (if a participant wishes to join a team or offer others to join, they can do so in the #ctf-st-elvis-teambuilding Discord Channel)

The maximum number of team members is five (5).

All teams must designate a Team Captain. A Team Captain serves as the official contact person for a team: this person should provide accurate and complete contact information to ensure that CTF organizers can reach their team if needed.

Each member of the team must be a registered participant in the CTF.

If participants choose to join a team, then they may not simultaneously participate as an individual or another team.

CHALLENGE SUBMISSIONS

All submissions must be received during the Challenge period. Submissions posted after the posted time frame will be disqualified.

Participants may get an answer but it will forfeit their points for that challenge. Even if the flag they tried before was similar. The decision to get the answer is final for zero points.

CHALLENGE SCORING

Each submission has set value known beforehand in the challenge description

The winning teams will be decided based on the number of the accumulated points during the CTF timeframe. In case two teams accumulate the same amount of points, the team that reached the amount of points in question faster will be the winner.

CHALLENGE DISQUALIFICATION

Whole team gets disqualified if any of the following applies:

- One or multiple team members have registered more than once
- One or multiple team members will not follow Code of Conduct (applies to any of the Biohacking village platforms or social media)

- Any offensive behaviour such as attacking the Biohacking Village infrastructure, denial of service, or escaping the boundaries set by the CTF or Device Lab environment

PRIVACY

Unless stated otherwise on the mainsite, we do not share any information about participants with anyone. Some events or conferences might have/require other rules, in that case it will be noted on the CTFd site.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Biohacking Village CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map

Description:

A scenario-driven Capture the Flag contest, pits teams of participants against adversaries and a clock, to protect human life and public safety. Participants compete against each other on both real and simulated medical devices, integrated into the fully immersive Biohacking Village: Device Lab, laid out as a working hospital.

Challenges will be tailored for all skill levels and draw from expertise areas including forensics, RF hacking, network exploitation techniques, web security, protocol reverse engineering, hardware hacking, and others. You will hack actual medical devices and play with protocols like DICOM, HL7 and FHIR.

2024 Capture the Flag Challenge

Welcome, elite hackers and cyber sleuths, to a CTF experience like no other - the "Code D.A.R.K. : Biohacking Village CTF Challenge".

Merge the worlds of biology and cybersecurity in an adrenaline-pumping contest that tests your skills in ways you've never imagined. Thrilling and challenging cybersecurity adventure centered around a hospital setting as a scenario where participants engage in a race against time to secure or retrieve critical medical data, navigating through various cybersecurity puzzles and challenges, where participants act as guardians of critical biological data.

Unravel Biological Mysteries: Dive into a narrative where biotechnology meets cyber-warfare. Decode genetic puzzles, breach virtual lab networks, and outsmart bioinformatics security systems.

Elevate Your Hacking Game: Challenge yourself with unique biocybersecurity scenarios. This isn't your typical CTF - it's a fusion of biotech intrigue and hardcore hacking.

Compete and Collaborate: Team up with fellow biohackers and cyber warriors. Share knowledge, strategize, and show off your skills in a community where biology and bits intersect.

Gear Up for a Cyber-Biotech Showdown

Immersive Scenarios: Each challenge is a step into a world where safeguarding biological data is as critical as securing digital assets.

Skill Diversity: Whether you're a veteran hacker or a biotech enthusiast, Code D.A.R.K. offers a range of puzzles that cater to a wide array of skills and interests.

- OT/IT
- Medical devices
- Hospital infrastructure
- Regulatory and international affairs
- Robotics
- Data
- **Mark your calendars** and set your alarms because the action kicks off on Friday, August 9th at 1000 PDT.
- **Play from anywhere in the world!** CTF open hours are as follows:
    - Friday, August 9th from 10am PST - 6pm PDT
    - Saturday, August 10th from 10am PST - 6pm PDT

♦ Sunday, August 11th from 10am PST - 12pm PDT

RULES

REGISTRATION

Participants may only register once for this challenge. If participants register for this challenge more than once, the whole teams with a participant that registered multiple times will be disqualified.

By registering, participants agree that their accounts may be rejected or terminated and all submissions by them and/or their Team may be disqualified if any of the information in their account is incorrect.

Participants must agree to and abide by the Code of Conduct while participating in the Biohacking Village Capture the Flag. Anyone who will conduct themselves against the CoC will be eliminated from competition and banned forever.

TEAMS

After participants register individually, they may work alone (team of one) or on one team with other challenge participants. To work on a team, they may either create a new team or join one that is pre-existing (if a participant wishes to join a team or offer others to join, they can do so in the #ctf-st-elvis-teambuilding Discord Channel)

The maximum number of team members is five (5).

All teams must designate a Team Captain. A Team Captain serves as the official contact person for a team: this person should provide accurate and complete contact information to ensure that CTF organizers can reach their team if needed.

Each member of the team must be a registered participant in the CTF.

If participants choose to join a team, then they may not simultaneously participate as an individual or another team.

CHALLENGE SUBMISSIONS

All submissions must be received during the Challenge period. Submissions posted after the posted time frame will be disqualified.

Participants may get an answer but it will forfeit their points for that challenge. Even if the flag they tried before was similar. The decision to get the answer is final for zero points.

CHALLENGE SCORING

Each submission has set value known beforehand in the challenge description

The winning teams will be decided based on the number of the accumulated points during the CTF timeframe. In case two teams accumulate the same amount of points, the team that reached the amount of points in question faster will be the winner.

CHALLENGE DISQUALIFICATION

Whole team gets disqualified if any of the following applies:

- One or multiple team members have registered more than once
- One or multiple team members will not follow Code of Conduct (applies to any of the Biohacking village platforms or social media)

- Any offensive behaviour such as attacking the Biohacking Village infrastructure, denial of service, or escaping the boundaries set by the CTF or Device Lab environment

PRIVACY

Unless stated otherwise on the mainsite, we do not share any information about participants with anyone. Some events or conferences might have/require other rules, in that case it will be noted on the CTFd site.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Biohacking Village CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map

Description:

A scenario-driven Capture the Flag contest, pits teams of participants against adversaries and a clock, to protect human life and public safety. Participants compete against each other on both real and simulated medical devices, integrated into the fully immersive Biohacking Village: Device Lab, laid out as a working hospital.

Challenges will be tailored for all skill levels and draw from expertise areas including forensics, RF hacking, network exploitation techniques, web security, protocol reverse engineering, hardware hacking, and others. You will hack actual medical devices and play with protocols like DICOM, HL7 and FHIR.

2024 Capture the Flag Challenge

Welcome, elite hackers and cyber sleuths, to a CTF experience like no other - the "Code D.A.R.K. : Biohacking Village CTF Challenge".

Merge the worlds of biology and cybersecurity in an adrenaline-pumping contest that tests your skills in ways you've never imagined. Thrilling and challenging cybersecurity adventure centered around a hospital setting as a scenario where participants engage in a race against time to secure or retrieve critical medical data, navigating through various cybersecurity puzzles and challenges, where participants act as guardians of critical biological data.

Unravel Biological Mysteries: Dive into a narrative where biotechnology meets cyber-warfare. Decode genetic puzzles, breach virtual lab networks, and outsmart bioinformatics security systems.

Elevate Your Hacking Game: Challenge yourself with unique biocybersecurity scenarios. This isn't your typical CTF - it's a fusion of biotech intrigue and hardcore hacking.

Compete and Collaborate: Team up with fellow biohackers and cyber warriors. Share knowledge, strategize, and show off your skills in a community where biology and bits intersect.

Gear Up for a Cyber-Biotech Showdown

Immersive Scenarios: Each challenge is a step into a world where safeguarding biological data is as critical as securing digital assets.

Skill Diversity: Whether you're a veteran hacker or a biotech enthusiast, Code D.A.R.K. offers a range of puzzles that cater to a wide array of skills and interests.

- OT/IT
- Medical devices
- Hospital infrastructure
- Regulatory and international affairs
- Robotics
- Data
- **Mark your calendars** and set your alarms because the action kicks off on Friday, August 9th at 1000 PDT.
- **Play from anywhere in the world!** CTF open hours are as follows:
    - Friday, August 9th from 10am PST - 6pm PDT
    - Saturday, August 10th from 10am PST - 6pm PDT

♦ Sunday, August 11th from 10am PST - 12pm PDT

RULES

REGISTRATION

Participants may only register once for this challenge. If participants register for this challenge more than once, the whole teams with a participant that registered multiple times will be disqualified.

By registering, participants agree that their accounts may be rejected or terminated and all submissions by them and/or their Team may be disqualified if any of the information in their account is incorrect.

Participants must agree to and abide by the Code of Conduct while participating in the Biohacking Village Capture the Flag. Anyone who will conduct themselves against the CoC will be eliminated from competition and banned forever.

TEAMS

After participants register individually, they may work alone (team of one) or on one team with other challenge participants. To work on a team, they may either create a new team or join one that is pre-existing (if a participant wishes to join a team or offer others to join, they can do so in the #ctf-st-elvis-teambuilding Discord Channel)

The maximum number of team members is five (5).

All teams must designate a Team Captain. A Team Captain serves as the official contact person for a team: this person should provide accurate and complete contact information to ensure that CTF organizers can reach their team if needed.

Each member of the team must be a registered participant in the CTF.

If participants choose to join a team, then they may not simultaneously participate as an individual or another team.

CHALLENGE SUBMISSIONS

All submissions must be received during the Challenge period. Submissions posted after the posted time frame will be disqualified.

Participants may get an answer but it will forfeit their points for that challenge. Even if the flag they tried before was similar. The decision to get the answer is final for zero points.

CHALLENGE SCORING

Each submission has set value known beforehand in the challenge description

The winning teams will be decided based on the number of the accumulated points during the CTF timeframe. In case two teams accumulate the same amount of points, the team that reached the amount of points in question faster will be the winner.

CHALLENGE DISQUALIFICATION

Whole team gets disqualified if any of the following applies:

- One or multiple team members have registered more than once
- One or multiple team members will not follow Code of Conduct (applies to any of the Biohacking village platforms or social media)

- Any offensive behaviour such as attacking the Biohacking Village infrastructure, denial of service, or escaping the boundaries set by the CTF or Device Lab environment

PRIVACY

Unless stated otherwise on the mainsite, we do not share any information about participants with anyone. Some events or conferences might have/require other rules, in that case it will be noted on the CTFd site.

Return to Index - Add to Google - ics Calendar file

BHV - Friday - 10:00-17:59 PDT

Title: Biohacking Village: Device Lab
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map

Description:

The Device Lab is highly-collaborative environment where security researchers test medical instruments, applications, and devices in real-time from participating Medical Device Manufacturers. Any potential issues are reported directly to the manufacturer, and coordinated vulnerability disclosures are produced.

As part of their product security programs, their proactive initiatives to test their products, and to enhance the cybersecurity of their medical technologies, select medical device makers are teaming up with the Biohacking Village.

These manufacturers are inviting security researchers to learn and to test their products in dedicated spaces set aside for them. Their staff will answer questions, educate researchers, and triage any potential security issues. Researchers who perform testing should expect to follow the manufacturers' published coordinated vulnerability disclosure policy and report any potential issues found so they can be addressed. Security researchers must sign the Hippocratic Oath for Hackers and agree to the framework of boundaries and rules of engagement during and post conference engagement.

We have 10 manufacturers with 21 devices. You can find more information about the devices and each manufacturer's Vulnerability Disclosure Policy here.

Return to Index - Add to Google - ics Calendar file

BHV - Saturday - 10:00-17:59 PDT

Title: Biohacking Village: Device Lab
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map

Description:

The Device Lab is highly-collaborative environment where security researchers test medical instruments, applications, and devices in real-time from participating Medical Device Manufacturers. Any potential issues are reported directly to the manufacturer, and coordinated vulnerability disclosures are produced.

As part of their product security programs, their proactive initiatives to test their products, and to enhance the cybersecurity of their medical technologies, select medical device makers are teaming up with the Biohacking Village.

These manufacturers are inviting security researchers to learn and to test their products in dedicated spaces set aside for them. Their staff will answer questions, educate researchers, and triage any potential security issues. Researchers who perform testing should expect to follow the manufacturers' published coordinated vulnerability disclosure policy and report any potential issues found so they can be addressed. Security researchers must sign the Hippocratic Oath for Hackers and agree to the framework of boundaries and rules of engagement during and post conference engagement.

We have 10 manufacturers with 21 devices. You can find more information about the devices and each manufacturer's Vulnerability Disclosure Policy here.

Return to Index - Add to Google - ics Calendar file

BHV - Sunday - 10:00-12:59 PDT

Title: Biohacking Village: Device Lab
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-07 - Map

Description:

The Device Lab is highly-collaborative environment where security researchers test medical instruments, applications, and devices in real-time from participating Medical Device Manufacturers. Any potential issues are reported directly to the manufacturer, and coordinated vulnerability disclosures are produced.

As part of their product security programs, their proactive initiatives to test their products, and to enhance the cybersecurity of their medical technologies, select medical device makers are teaming up with the Biohacking Village.

These manufacturers are inviting security researchers to learn and to test their products in dedicated spaces set aside for them. Their staff will answer questions, educate researchers, and triage any potential security issues. Researchers who perform testing should expect to follow the manufacturers' published coordinated vulnerability disclosure policy and report any potential issues found so they can be addressed. Security researchers must sign the Hippocratic Oath for Hackers and agree to the framework of boundaries and rules of engagement during and post conference engagement.

We have 10 manufacturers with 21 devices. You can find more information about the devices and each manufacturer's Vulnerability Disclosure Policy here.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-16:59 PDT

Title: Blacks in Cyber CTF
When: Friday, Aug 9, 12:00 - 16:59 PDT
Where: Virtual

Description:

Hybrid Contest Contest available online Friday 12:00 to Saturday 17:00

The BIC Village Capture The Flag is a jeopardy style event designed to practice solving challenges in multiple categories. This event seeks to not only be a series of puzzles and challenges to solve, but a gamified way to learn concepts of social justice and Black history. This event will highlight previous, current and up & coming Black individuals and their contributions to technology. This year we are excited to bring back our physical challenge room with a variety of interactive components for players to interface with.

This event also aims to bring to the forefront a range of technologies that we will expose to the community that operate in our day-to-day lives and examine their capabilities; contributing to the discussion of privacy, social justice and civil rights. Our event will allow the DEF CON community to fully engage in “Reading all the stories, learning all the technologies, and hacking all the things.”

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-16:59 PDT

Title: Blacks in Cyber CTF
When: Saturday, Aug 10, 10:00 - 16:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Hybrid Contest Contest available online Friday 12:00 to Saturday 17:00

The BIC Village Capture The Flag is a jeopardy style event designed to practice solving challenges in multiple categories. This event seeks to not only be a series of puzzles and challenges to solve, but a gamified way to learn concepts of social justice and Black history. This event will highlight previous, current and up & coming Black individuals and their contributions to technology. This year we are excited to bring back our physical challenge room with a variety of interactive components for players to interface with.

This event also aims to bring to the forefront a range of technologies that we will expose to the community that operate in our day-to-day lives and examine their capabilities; contributing to the discussion of privacy, social justice and civil rights. Our event will allow the DEF CON community to fully engage in “Reading all the stories, learning all the technologies, and hacking all the things.”

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-17:59 PDT

Title: Blacks in Cyber CTF
When: Friday, Aug 9, 12:00 - 17:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Hybrid Contest Contest available online Friday 12:00 to Saturday 17:00

The BIC Village Capture The Flag is a jeopardy style event designed to practice solving challenges in multiple categories. This event seeks to not only be a series of puzzles and challenges to solve, but a gamified way to learn concepts of social justice and Black history. This event will highlight previous, current and up & coming Black individuals and their contributions to technology. This year we are excited to bring back our physical challenge room with a variety of interactive components for players to interface with.

This event also aims to bring to the forefront a range of technologies that we will expose to the community that operate in our day-to-day lives and examine their capabilities; contributing to the discussion of privacy, social justice and civil rights. Our event will allow the DEF CON community to fully engage in “Reading all the stories, learning all the technologies, and hacking all the things.”

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-17:59 PDT

Title: Blacks in Cyber CTF
When: Friday, Aug 9, 12:00 - 17:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

The BIC Village Capture The Flag is a jeopardy style event designed to practice solving challenges in multiple categories. This event seeks to not only be a series of puzzles and challenges to solve, but a gamified way to learn concepts of social justice and Black history. This event will highlight previous, current and up & coming Black individuals and their contributions to technology. This year we are excited to bring back our physical challenge room with a variety of interactive components for players to interface with.

This event also aims to bring to the forefront a range of technologies that we will expose to the community that operate in our day-to-day lives and examine their capabilities; contributing to the discussion of privacy, social justice and civil rights. Our event will allow the DEF CON community to fully engage in “Reading all the stories, learning all the technologies, and hacking all the things.”

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-16:59 PDT

Title: Blacks in Cyber CTF
When: Saturday, Aug 10, 10:00 - 16:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

The BIC Village Capture The Flag is a jeopardy style event designed to practice solving challenges in multiple categories. This event seeks to not only be a series of puzzles and challenges to solve, but a gamified way to learn concepts of social justice and Black history. This event will highlight previous, current and up & coming Black individuals and their contributions to technology. This year we are excited to bring back our physical challenge room with a variety of interactive components for players to interface with.

This event also aims to bring to the forefront a range of technologies that we will expose to the community that operate in our day-to-day lives and examine their capabilities; contributing to the discussion of privacy, social justice and civil rights. Our event will allow the DEF CON community to fully engage in “Reading all the stories, learning all the technologies, and hacking all the things.”

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-16:59 PDT

Title: Blacks in Cyber CTF
When: Friday, Aug 9, 12:00 - 16:59 PDT
Where: Virtual

Description:

The BIC Village Capture The Flag is a jeopardy style event designed to practice solving challenges in multiple categories. This event seeks to not only be a series of puzzles and challenges to solve, but a gamified way to learn concepts of social justice and Black history. This event will highlight previous, current and up & coming Black individuals and their contributions to technology. This year we are excited to bring back our physical challenge room with a variety of interactive components for players to interface with.

This event also aims to bring to the forefront a range of technologies that we will expose to the community that operate in our day-to-day lives and examine their capabilities; contributing to the discussion of privacy, social justice and civil rights. Our event will allow the DEF CON community to fully engage in “Reading all the stories, learning all the technologies, and hacking all the things.”

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 19:00-01:59 PDT

Title: Blacks in Cyber Lituation 2.0
When: Friday, Aug 9, 19:00 - 01:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:
19: 00 - 21:00
BIC Village "Chat & Chew" Networking Session
Light Music & Food! Network with our sponsors, partners, volunteers, members and visitors!

21:00 - 02:00 BIC Village Party with DJ Roma As the sun sets, gather around for a celebration of Reggae, Soca, Dancehall, Hiphop, Pop, R&B, Regional Hits and Caribbean Dance Style! All Flags Welcome! Rep Your Flag!

Speakers:BIC Village Staff,DJ Roma

SpeakerBio: BIC Village Staff
No BIO available
SpeakerBio: DJ Roma
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 19:00-00:59 PDT

Title: BlanketFort Con
When: Friday, Aug 9, 19:00 - 00:59 PDT
Where: LVCC West/Floor 3/W305-W306 - Map

Description:

BlanketFort Con: Come for the chill vibes and diversity, stay for the Blanket Fort Building, Cool Lights, Music, and Kid Friendly \ Safe environment. Now with less Gluten and more animal onesies!

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 17:15-17:59 PDT

Title: Bloch Party & More Debates
When: Saturday, Aug 10, 17:15 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

Title: Blue Goes Purple: Purple Teams for Fun and Profit (A BTV & RTV Panel)
When: Friday, Aug 9, 16:00 - 16:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

This panel will consist of leaders and practitioners from multiple areas of the security and hacking space, working together to unite the Red Team and the Blue Team.

Speakers: Catherine J. Ullman,Jake Williams,Meaghan Neill,Ralph May,Matthew Nickerson

SpeakerBio: Catherine J. Ullman, Principle Technology Architect, Security at University at Buffalo

Dr. Catherine J. Ullman is a security researcher, speaker, author, and Principal Technology Architect, Security, at the University at Buffalo with over 20 years of highly technical experience. In her current role, Cathy is a digital forensics and incident response (DFIR) specialist, performing incident management, intrusion detection, investigative services, and personnel case resolution in a dynamic academic environment. She additionally builds security awareness among faculty and staff which educates and informs users about how to prevent and detect social engineering threats, and how to compute and digitally communicate safely. Cathy has presented at numerous information security conferences including DEF CON and Blue Team Con. Cathy is a contributor to the O'Reilly title 97 Things Every Information Professional Should Know and the author of the Wiley title The Active Defender. In her (minimal) spare time, she enjoys visiting her adopted two-toed sloth Flash at the Buffalo Zoo, researching death and the dead, and learning more about hacking things to make the world a more secure place.

SpeakerBio: Jake Williams
No BIO available

SpeakerBio: Meaghan Neill, Threat Hunter and DFIR Analyst at EY Canada

Meaghan is a Threat Hunter and DFIR Analyst with EY Canada's MDR department. She currently holds her BSc in Computer Science, with a specialization in Systems and Information Security from MacEwan University and her GCFA. While at EY, her focus has been in Threat Hunting, Digital Forensics, Incident Response, Adversary Emulation, and Purple Teaming.

SpeakerBio: Ralph May, Security Analyst and Penetration Tester at Black Hills Information Security (BHIS)

Ralph is a security analyst and penetration tester at Black Hills Information Security. Ralph is also a co-developer and instructor of the Practical Physical Exploitation course. Before joining BHIS, Ralph spent five years performing offensive operations on a wide range of security assessments. These assessments include physical, wireless, network, social engineering, and full simulation red teams. Before focusing on security, Ralph worked as a system administrator and network engineer for civilian and government employers. Ralph is a US Army veteran who previously worked with the United States Special Operations Command (USSOCOM) on information security challenges and threat actor simulations.

SpeakerBio: Matthew Nickerson
No BIO available

Return to Index - Add to Google - ics Calendar file

BTV - Sunday - 10:30-11:59 PDT

Title: Blue Team Careers: Do what you love, get paid for it! (A BTV Interactive Panel)
When: Sunday, Aug 11, 10:30 - 11:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

This panel will consist of leaders and practitioners from multiple areas of the security and hacking space, sharing their journeys and perspectives on the industry. They'll answer your questions on hiring, career advancement, and technical growth. Join us for this interactive session!

This panel will consist of leaders and practitioners from multiple areas of the security and hacking space, sharing their journeys and perspectives on the industry. They'll answer your questions on hiring, career advancement, and technical growth. Join us for this interactive session!

Speakers: Cyb0rg42,Dani,Shea Nangle,Tennisha Martin,Pete Ortega

SpeakerBio: Cyb0rg42
No BIO available
SpeakerBio: Dani

With more than 10 years in different security roles, last 5 years in the current role has brought me in the position to be the security department education advisor. I believe education and career path advice should be the role for a technical professional and not HR. It is important to know both the hunger for education and the pain of going through heavy learning curve. But it is also important to underatand the need to slow down at times for other life events. Also, helping eachother builds life long friendships and trust.

SpeakerBio: Shea Nangle
No BIO available
SpeakerBio: Tennisha Martin

Tennisha Martin is the founder and Executive Director of BlackGirlsHack (BGH Foundation), a national cybersecurity nonprofit organization dedicated to providing education and resources to underserved communities and increasing the diversity in cyber. BlackGirlsHack provides its members with resources, mentorship, direction, and training required to enter and excel in the cybersecurity field. Tennisha has a bachelor's degree in Electrical and Computer Engineering from Carnegie Mellon University and several Master's Degrees including in Cybersecurity and Business Administration. She has worked in a consulting capacity for over 15 years and is a best selling author, award winning hacker, and an advocate for diversity.

SpeakerBio: Pete Ortega
No BIO available

Return to Index - Add to Google - ics Calendar file

BTV - Sunday - 12:00-12:30 PDT

Title: Blue Team Village Closing Ceremonies
When: Sunday, Aug 11, 12:00 - 12:30 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

This is a placeholder for BTV's closing ceremonies!

This is a placeholder for BTV's closing ceremonies! This is a placeholder for BTV's closing ceremonies! This is a placeholder for BTV's closing ceremonies! This is a placeholder for BTV's closing ceremonies! This is a placeholder for BTV's closing ceremonies! This is a placeholder for BTV's closing ceremonies!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:30-17:59 PDT

Title: Blue Team Village CTF
When: Saturday, Aug 10, 10:30 - 17:59 PDT
Where: LVCC West/Floor 3/W311-W313 - Map

Description:

In-Person Contest Friday and Saturday: 10:30-18:00 CTF begins Friday 10:30; CTF ends Saturday 18:00

The Blue Team Village (BTV) CTF is a cyber defense Capture the Flag inspired by a mix of trending nation-state actor kill chains and at least one custom insider threat story. You are an incident responder tasked to investigate several incidents involving different operating systems and OT devices. You will have access to SIEM and Packet captures; however, just like in real life, these tools have issues you must overcome to uncover what happened.

Expect indexes to telemetry issues, raw data not extracted properly, and missing fields. Regex may be helpful. In addition, Arkime, the network monitoring tool, will only work partially and correctly. You must find ways to make the best of the telemetry provided, and remember that you can always extract the resulting pcaps!

The CTF challenges contestants to leverage diverse cyber defense skills, including Incident Response, Forensics, and Threat Hunting. Both host and network telemetry are required to solve all the flags.

BTV's Project Obsidian crew developed the CTF to allow anyone, regardless of skill or knowledge, to participate and sharpen their cyber defense skills. We recommend creating or joining a team if you are new to cyber defense. We highly recommend participating in the BTV's Project Obsidian workshop sessions if you are new to cyber defense. Sessions cover many of the topics on the CTF and will help you along the way.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:30-17:59 PDT

Title: Blue Team Village CTF
When: Friday, Aug 9, 10:30 - 17:59 PDT
Where: LVCC West/Floor 3/W311-W313 - Map

Description:

In-Person Contest Friday and Saturday: 10:30-18:00 CTF begins Friday 10:30; CTF ends Saturday 18:00

The Blue Team Village (BTV) CTF is a cyber defense Capture the Flag inspired by a mix of trending nation-state actor kill chains and at least one custom insider threat story. You are an incident responder tasked to investigate several incidents involving different operating systems and OT devices. You will have access to SIEM and Packet captures; however, just like in real life, these tools have issues you must overcome to uncover what happened.

Expect indexes to telemetry issues, raw data not extracted properly, and missing fields. Regex may be helpful. In addition, Arkime, the network monitoring tool, will only work partially and correctly. You must find ways to make the best of the telemetry provided, and remember that you can always extract the resulting pcaps!

The CTF challenges contestants to leverage diverse cyber defense skills, including Incident Response, Forensics, and Threat Hunting. Both host and network telemetry are required to solve all the flags.

BTV's Project Obsidian crew developed the CTF to allow anyone, regardless of skill or knowledge, to participate and sharpen their cyber defense skills. We recommend creating or joining a team if you are new to cyber defense. We highly recommend participating in the BTV's Project Obsidian workshop sessions if you are new to cyber defense. Sessions cover many of the topics on the CTF and will help you along the way.

Return to Index - Add to Google - ics Calendar file

CHV - Friday - 15:00-15:30 PDT

Title: Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack
When: Friday, Aug 9, 15:00 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

In this talk, I will detail my discovery and analysis of CVE 2023-52709, a vulnerability in the TI Bluetooth stack. This flaw allows the stack to fail in generating a resolvable Random Private Address (RPA), which can lead to a Denial of Service (DoS) for already bonded peer devices. The discussion will cover the technical aspects of the vulnerability, the implications for automotive security, and potential mitigation strategies.

SpeakerBio: Kevin Mitchell

Kevin Mitchell is an innovative architect and cybersecurity expert renowned for uncovering vulnerabilities in embedded systems. With a background in hardware and software security, Kevin identified CVE-2023-52709, a flaw in the TI Bluetooth stack leading to potential DoS attacks. His work underscores his expertise in safeguarding interconnected devices. A regular at DEFCON's Car Hacking Village, Kevin is dedicated to enhancing the security of modern automotive systems.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 10:00-11:45 PDT

Title: Bluetooth Landscape Exploration & Enumeration Platform (BLEEP)
When: Friday, Aug 9, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W306 - Map

Description:

The purpose of the tool platform is to provide both novice and experienced Bluetooth researchers a “swiss-army knife” for device exploration and enumeration. The Bluetooth Landscape Exploration & Enumeration Platform (BLEEP) is capable of discovering Bluetooth Low Energy (BLE) devices, connecting to them, and enumerating the device as well. BLEEP leverages Python3, BlueZ, and the Linux D-Bus to provide a terminal user interface for identifying and interacting with BLE implements. The I/O capabilities of the toolset include read I/O, performing writes, and capturing of notification signals. The purpose of using these low-level libraries is to maintain small granularity control over the interactivity between BLEEP and the BLE environment.

SpeakerBio: Paul Wortman

Dr. Wortman has a PhD in Electrical and Computer Engineering from the University of Connecticut with research that ranged from network analysis to cyber security risk evaluation. He now focuses on Bluetooth protocol and devices research.

Return to Index - Add to Google - ics Calendar file

Title: BOAZ, Yet Another layered Evasion Tool: Unveiling the Secrets Behind Antivirus Testing
When: Saturday, Aug 10, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

Antivirus (AV) solutions, serving as the last line of defense on users' endpoint devices, have evolved into highly complex entities. Often operated as 'black boxes' from user's perspective due to proprietary and security reasons, the principle of 'security through obscurity' - though far from ideal - remains prevalent in the cat-and-mouse game between defenders and attackers. This dynamic places researchers and attackers in similar positions; while malware authors can fingerprint AV detection mechanisms through various evasion techniques, researchers can employ similar methods to identify improvement opportunities in security products. This study evaluates the effectiveness and performance of AV solutions against 18 open-source evasion frameworks. Notably, no AV solution could detect all samples from open-source evasion tools, and conversely, no evasion tool could bypass all contemporary AVs. This limitation is primarily attributed to the AVs' reliance on signature and heuristic engines to balance between performance, security and access (false-positive rates). To delve deeper into AV detection capabilities across signature, heuristic, and behavioral evasions, we built BOAZ - an evasion tool serving both as a research instrument and an evasion framework. Through empirical experimentation, our findings reveal not only the varied performance of AV solutions against different evasion frameworks and techniques but also the potential for strategically combining these techniques to penetrate secured environments without needing commercial tools or zero-day exploits. Effectively, by understanding the building blocks of AV detection and evasion phases, anyone can develop their own evasion tool.

SpeakerBio: Thomas X Meng
No BIO available

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 13:30-13:59 PDT

Title: Bogus Badges: The Art and Innovation of Badge Counterfeiting
When: Friday, Aug 9, 13:30 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Counterfeiting badges for conferences and employee access has evolved into a sophisticated craft, blending creativity with technology. This talk explores modern techniques from traditional methods to innovations like 3D printing and digital replication. We uncover how these tools enable counterfeiting to compromise even highly secure systems.

SpeakerBio: Nick Warner

Nick is a Penetration Testing Consultant for the Secureworks Adversary Group, specializing in identifying and exploiting security vulnerabilities to help organizations strengthen their defenses. He is also a 3D printing enthusiast, particularly adept at combining technological creativity with practical applications. This unique blend of skills enables him to approach security challenges from diverse and inventive perspectives.

Return to Index - Add to Google - ics Calendar file

Title: BOLABuster: Harnessing LLMs for Automating BOLA Detection
When: Friday, Aug 9, 11:30 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Broken Object Level Authorization (BOLA) is a prevalent vulnerability in modern APIs and web applications, ranked as the top risk in the OWASP API top 10 and the fourth most reported vulnerability type in HackerOne Global Top 10. The consequences of BOLA can be severe, from sensitive data exposure to a total loss of system control.

While manually verifying or triggering known BOLAs is typically straightforward, automatically identifying the correct execution sequences and generating viable input values for testing BOLAs is challenging. The complexities of application and business logic, the wide range of input parameters, and the stateful nature of modern web applications all hinder existing static analysis tools from detecting unknown BOLAs.

To overcome these challenges, we leverage LLM's reasoning and generative capabilities to automate tasks that were previously done manually. These tasks include understanding application logic, uncovering endpoint dependency relationships, generating test cases, and interpreting test results. When combined with heuristics, this AI-backed method enables fully automated BOLA detection at scale. We dub this research BOLABuster.

Although BOLABuster is still in its early stages, it has already discovered multiple new vulnerabilities in open-source projects. In one instance, we submitted 15 CVEs for one project, some leading to critical privilege escalation. Our most recent disclosed vulnerability was CVE-2024-1313, a BOLA vulnerability in Grafana, an open-source project used by over 20 million users.

When benchmarked against other state-of-the-art fuzzing tools using applications with known BOLAs, BOLABuster, on average, sends less than 1% of the API requests to a target server to uncover a BOLA.

In this talk, we will share our methodology and the lessons learned from our research. We invite you to join us to learn about our journey with AI and explore a new approach to conducting vulnerability research.

Speakers:Ravid Mazon,Jay Chen

SpeakerBio: Ravid Mazon

Ravid:
Ravid is a Senior Security Researcher at Palo Alto Networks with more than 6 years of hands-on experience in the Application & API Security field. As a Bachelor of Information Systems with a specialization in Cyber, Ravid brings an innovative attitude to the table, while researching different aspects in the AppSec world. He's eager to experience, experiment, and learn something new every day. In his free time, Ravid likes to travel, exercise, and have a good time with friends and family.

Jay: Jay Chen is a Cloud Security Researcher with Prisma Cloud and Unit 42 at Palo Alto Networks. He has extensive research experience in cloud security. In his role at Palo Alto Networks, he focuses on investigating the vulnerabilities, design flaws, and adversarial TTPs in cloud-native technologies such as containers and public cloud services. He works to develop methodologies for identifying and remediating security gaps in public clouds and works to protect Prisma customers from threats.

SpeakerBio: Jay Chen

Jay Chen is a Cloud Security Researcher with Prisma Cloud and Unit 42 at Palo Alto Networks. He has extensive research experience in cloud security. In his role at Palo Alto Networks, he focuses on investigating the vulnerabilities, design flaws, and adversarial TTPs in cloud-native technologies such as containers and public cloud services. He works to develop

methodologies for identifying and remediating security gaps in public clouds and works to protect Prisma Cloud customers from threats.

In previous roles, he has researched mobile cloud security and distributed storage security. Jay has authored 25+ academic and industrial papers.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 11:00-11:30 PDT

Title: BOLABuster: Harnessing LLMs for Automating BOLA Detection
When: Saturday, Aug 10, 11:00 - 11:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

BOLA is a prevalent vulnerability in modern APIs and web applications, topping the OWASP API risk chart, and ranking fourth in HackerOne Global Top 10. Its impact ranges from data exposure to total system control loss.

While manually triggering known BOLAs is relatively straightforward, automatic detection is challenging due to the complexities of application logic, the wide range of inputs, and the stateful nature of modern web applications.

To tackle this, we leveraged LLMs to automate manual tasks such as understanding application logic, revealing endpoint dependency relationships, generating test cases, and interpreting results. Our AI-backed approach enables automating BOLA detection at scale, named BOLABuster.

Though in its early stages, BOLABuster identified numerous vulnerabilities in open-source projects. In one case, we submitted 15 CVEs for a project, some leading to critical privilege escalation. Our latest disclosed vulnerability was CVE-2024-1313, a BOLA in Grafana,

Speakers:
Jay Chen,Ravid Mazon

SpeakerBio: Jay Chen

Jay Chen is a Cloud Security Researcher with Prisma Cloud and Unit 42 at Palo Alto Networks. He has extensive research experience in cloud security. In his role at Palo Alto Networks, he focuses on investigating the vulnerabilities, design flaws, and adversarial TTPs in cloud-native technologies such as containers and public cloud services. He works to develop methodologies for identifying and remediating security gaps in public clouds and works to protect Prisma Cloud customers from threats.

In previous roles, he has researched mobile cloud security and distributed storage security. Jay has authored 25+ academic and industrial papers.

SpeakerBio: Ravid Mazon

Ravid:
Ravid is a Senior Security Researcher at Palo Alto Networks with more than 6 years of hands-on experience in the Application & API Security field. As a Bachelor of Information Systems with a specialization in Cyber, Ravid brings an innovative attitude to the table, while researching different aspects in the AppSec world. He’s eager to experience, experiment, and learn something new every day. In his free time, Ravid likes to travel, exercise, and have a good time with friends and family.

Jay: Jay Chen is a Cloud Security Researcher with Prisma Cloud and Unit 42 at Palo Alto Networks. He has extensive research experience in cloud security. In his role at Palo Alto Networks, he focuses on investigating the vulnerabilities, design flaws, and adversarial TTPs in cloud-native technologies such as containers and public cloud services. He works to develop methodologies for identifying and remediating security gaps in public clouds and works to protect Prisma customers from threats.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 14:00-14:45 PDT

Title: Book Signing: Visual Threat Intelligence: An Illustrated Guide for Threat Researchers
When: Friday, Aug 9, 14:00 - 14:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:

The first 35 Veterans can receive a free autographed vopy of Mr Roccia's new book, Visual Threat Intelligence: An Illustrated Guide for Threat Researchers, courtesy of VETCON.

SpeakerBio: Thomas Roccia, Senior Security Researcher at Microsoft

Thomas Roccia is working as a Senior Security Researcher at Microsoft and works on malware research, generative AI and threat intelligence. In addition to his work at Microsoft, Thomas also runs SecurityBreak, an online platform where he showcases his latest projects and research findings.

Thomas has travelled the world to manage critical outbreaks and has been on the front lines of some of the most well-known threats. He has tracked cybercrime and nation-state campaigns and has worked closely with law enforcement agencies.

In addition to his professional work, Thomas is a regular speaker at security conferences and is committed to contributing to the open-source community through various projects. He runs the Unprotect Project, an open malware evasion techniques database, since 2015. He is also the author of the book Visual Threat Intelligence, an illustrated guide for threat researchers. Thomas's work has been quoted by multiple media outlets around the world.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 11:30-17:30 PDT

Title: Book Signings
When: Friday, Aug 9, 11:30 - 17:30 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-04 - Map

Description:

Book Signing Schedule

Friday, August 9 11:30 a.m. Tim Arnold, Black Hat Python, 2nd Edition 12:00 p.m. Jack Rhysider from Darknet Diaries 12:30 p.m. James Forshaw, Windows Security Internals 1:30 p.m. Nick Aleks, Black Hat Bash [DEF CON edition] and Black Hat GraphQL 2:30 p.m. Jim O'Gorman and Daniel Graham, Metasploit, 2nd Edition [DEF CON edition] 3:30 p.m. Corey Ball, Hacking APIs 4:30 p.m. Elonka Dunin and Klaus Schmeh, Codebreaking

Saturday, August 10 10:30 a.m. Travis Goodspeed, Microcontroller Exploitsand PoC||GTFO, Volumes 1, 2, and 3 12:30 p.m. Micah Lee, Hacks, Leaks, and Revelations 1:30 p.m. Jon DiMaggio, The Art of Cyberwarfare 2:30 p.m. Matt Burrough and Jos Weyers, Locksport 3:30 p.m. Chris Eagle and Kara Nance, The Ghidra Book 4:30 p.m. Alex Matrosov, Rootkits and Bootkits

Sunday, August 11 11:30 a.m. Beau Woods, Fotios Chantzis, and Paulino Calderon, Practical IoT Hacking

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Botnets
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Join us for an interactive workshop where we will walk you through the ins and outs of botnet deployment and operation via a command and control web server. Geared towards beginners, this workshop offers a hands-on approach to understanding how botnets function. You'll also learn an effective defense strategy against the botnet you have created. No experience needed we will give you everything you need!

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Botnets
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Join us for an interactive workshop where we will walk you through the ins and outs of botnet deployment and operation via a command and control web server. Geared towards beginners, this workshop offers a hands-on approach to understanding how botnets function. You'll also learn an effective defense strategy against the botnet you have created. No experience needed we will give you everything you need!

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Botnets
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Join us for an interactive workshop where we will walk you through the ins and outs of botnet deployment and operation via a command and control web server. Geared towards beginners, this workshop offers a hands-on approach to understanding how botnets function. You'll also learn an effective defense strategy against the botnet you have created. No experience needed we will give you everything you need!

Return to Index - Add to Google - ics Calendar file

DC - Friday - 14:30-15:15 PDT

Title: Breaching AWS Accounts Through Shadow Resources
When: Friday, Aug 9, 14:30 - 15:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

The cloud seems complex, but it's what happens behind the scenes that really complicates things. Some services utilize others as resources as part of their logic/operation. Interestingly enough, it turns out that this could lead to catastrophic results if done unsafely.

This talk will present six critical vulnerabilities that we found in AWS, along with the stories and methodologies behind them. These vulnerabilities, which were all promptly acknowledged and fixed by AWS, could allow external attackers to breach almost any AWS account. The vulnerabilities range from remote code execution, which could lead to full account takeover, to information disclosure, potentially exposing sensitive data, or causing denial of service. The session will share our story of discovery, how we were able to identify commonalities among them, and how we developed a method to uncover more vulnerabilities and enhance the impact by using common techniques leading to privilege escalation. We will then detail our approach for mapping service external resources and release our Open-Source tool to research service internal API calls. We will also present a method to check if accounts have been vulnerable to this vector in the past.

We will conclude our talk with the lessons learned during this research and our future line of research. We will highlight new areas that cloud researchers need to explore when hunting for cloud vulnerabilities and highlight best practices for developers to use in complex environments.

- link
- link
- link

Speakers: Yakir Kadkoda,Michael Katchinskiy,Ofek Itach

SpeakerBio: Yakir Kadkoda, Lead Security Researcher, Team Nautilus at Aqua

Yakir Kadkoda is a Lead Security Researcher at Aqua's research team, Team Nautilus. He combines his expertise in vulnerability research with a focus on discovering and analyzing new security threats and attack vectors in cloud native environments, supply chain security, and CI/CD processes. Prior to joining Aqua, Yakir worked as a red teamer. Yakir has shared his cybersecurity insights at major industry events like Black Hat and RSA.

SpeakerBio: Michael Katchinskiy

Michael Katchinskiy is a Security Researcher and a Computer Science student at the Technion. His work focuses on researching and analyzing new attack vectors in cloud-native environments, specializing in Kubernetes and integrating CNAPP data to detect and prevent attacks.

SpeakerBio: Ofek Itach, Senior Security Researcher at Aqua

Ofek Itach is a Senior Security Researcher at Aqua, specializing in cloud research. His work centers on identifying and analyzing attack vectors in cloud environments, enhancing security measures for cloud platforms and cloud environments.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 11:00-11:40 PDT

Title: Breaking and Defending Cloud Infrastructure: Red Team Evasion Tactics and Access Control Solutions
When: Saturday, Aug 10, 11:00 - 11:40 PDT
Where: Virtual

Description:
Speakers: Amal Joy,Abhishek S

SpeakerBio: Amal Joy, Security Engineer at Highradius

Amal Joy is a Security Engineer at Highradius. His area of research falls into Infrastuture Security , Redteaming in Multicloud environments and Corporate Networks. He also loves spending leasure time on malware development. He is an Executive member of DC0471 defcon group He has over 3 years of experience in playing CTF's and also hosted many hiring MultiCloud Adversary CTF's in Reputed conferences like Seasides 22. With Strong focus on MultiCloud and ActiveDirectory, He currently holds various certifications like CARTP,MCRTA,CCRTA,EJPT.

SpeakerBio: Abhishek S, Security Engineer at Flipkart

Abhishek S is a Security Engineer at Flipkart with primary research focus in application security and red teaming. He is a staff of Adversary Village at (DEF CON) and an executive member of DC0471 group, he has been a speaker for various conferences like C0c0n 23 and Blackhat MEA 23. With over 4 years of experience playing CTF(s) and hunting for vulnerabilities in various VDP programs. He is listed in hall of fames of Google, Facebook, Microsoft and 40+ organizations for finding their security vulnerabilities. He has about four cve(s) from various organizations such as Android, Tenable, StrAPI CMS etc. currently holds various certifications such as OSCP, BSCP, CRTP, GIAC GFACT etc. Other than the technical side, he loves to travel around the world and is a automotive enthusiast.

Return to Index - Add to Google - ics Calendar file

BHV - Friday - 15:00-15:30 PDT

Title: Breaking Boundaries: Popping Shells in the Airgap with $10 and a Dash of Arduino Magic
When: Friday, Aug 9, 15:00 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Many medical devices are “not connected to a network”, so let’s bring our own! This talk will teach you how to create a BadUSB device that can wirelessly execute payloads on “airgapped” systems like medical devices that aren’t connected to the internet. WIth only $10 of off-the-shelf hardware and some basic arduino code you too can start popping shells in the device lab.

SpeakerBio: Daniel Beard

Daniel is a software engineer and entrepreneur specializing in medical device cybersecurity. He founded MedISAO and Cyberprotek, both acquired by MedCrypt in 2020. His expertise includes vulnerability management, and designing secure devices in a regulated environment.

Return to Index - Add to Google - ics Calendar file

Title: Breaking Secure Web Gateways (SWG) for Fun and Profit
When: Friday, Aug 9, 17:00 - 17:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Secure Web Gateways (SWGs) are cloud-based SSL-intercepting proxies and an important component of enterprise Secure Access Service Edge (SASE) or Security Service Edge (SSE) solutions. SWGs ensure secure web access for enterprise users by doing malware protection, threat prevention, URL filtering, and content inspection of sensitive data, among other critical security measures.

Our research indicates that in today's world of complex web applications and protocols, SWGs often fail to deliver on their promise. We will demonstrate a new class of attacks: “Last Mile Reassembly Attacks,” which, as of this writing, can bypass every SWG in the Gartner Magic Quadrant for SASE and SSE - this includes the largest public market cybersecurity companies in the world. Additionally, we will release an open-source attack toolkit for researchers and red teams to test these attacks on their security solutions and better understand their security exposure.

We aim for our talk to compel SWG vendors to rethink cloud-based client-side web attack detection models, and for enterprises to rethink how they look at securing their users against web threats.

Secure Web Gateway Basics: link SSL Interception and Attacks: link

Speakers:
Vivek Ramachandran,Jeswin Mathai

SpeakerBio: Vivek Ramachandran, Founder at SquareX

Vivek Ramachandran is a security researcher, book author, speaker-trainer, and serial entrepreneur with over two decades of experience in offensive cybersecurity. He is currently the founder of SquareX, building a browser-native security product focused on detecting, mitigating, and threat-hunting web attacks against enterprise users and consumers. Prior to that, he was the founder of Pentester Academy (acquired in 2021), which has trained thousands of customers from government agencies, Fortune 500 companies, and enterprises from over 140+ countries. Before that, Vivek’s company built an 802.11ac monitoring product sold exclusively to defense agencies. Vivek discovered the Caffe Latte attack, broke WEP Cloaking, conceptualized enterprise Wi-Fi Backdoors, and created Chellam (Wi-Fi Firewall), WiMonitor Enterprise (802.11ac monitoring), Chigula (Wi-Fi traffic analysis via SQL), Deceptacon (IoT Honeypots), among others. He is the author of multiple five-star-rated books in offensive cybersecurity, which have sold thousands of copies worldwide and have been translated into multiple languages. He has been a speaker/trainer at top security conferences such as Blackhat USA, Europe and Abu Dhabi, DEFCON, Nullcon, Brucon, HITB, Hacktivity, and others. Vivek’s work in cybersecurity has been covered in Forbes, TechCrunch, and other popular media outlets. In a past life, he was one of the programmers of the 802.1x protocol and Port Security in Cisco’s 6500 Catalyst series of switches. He was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. He has also published multiple research papers in the field of DDoS, ARP Spoofing Detection, and Anomaly-based Intrusion Detection Systems. In 2021, he was awarded an honorary title of Regional Director of Cybersecurity by Microsoft for a period of three years, and in 2024 he joined the BlackHat Arsenal Review Board.

SpeakerBio: Jeswin Mathai, Chief Architect at SquareX

Jeswin Mathai serves as the Chief Architect at SquareX, where he leads the design and implementation of the company's infrastructure. Before joining SquareX, he was part of Pentester Academy (acquired by INE) where he was responsible for managing the whole lab platform that was used by thousands of customers from government agencies, Fortune 500 companies, and enterprises from over 140+ countries. A seasoned speaker and researcher, Jeswin has showcased his work at prestigious international stages such as DEFCON China, RootCon, Blackhat Arsenal, and Demo Labs at DEFCON. He has

also imparted his knowledge globally, training in-classroom sessions at Black Hat US, Asia, HITB, RootCon, and OWASP NZ Day. Jeswin is also the creator of popular open-source projects such as AWSGoat, AzureGoat, and PAToolkit. He holds a Bachelor's degree from IIIT Bhubaneswar, where he led the InfoSec Society. In association with CDAC and ISEA, he spearheaded security audits of government portals and orchestrated cybersecurity workshops for government officials. Jeswin's professional interests are focused on advancing the fields of Cloud Security, Container Security, and Browser Security.

Return to Index - Add to Google - ics Calendar file

PYV - Saturday - 13:00-13:59 PDT

Title: Breaking software protected crypto implementations
When: Saturday, Aug 10, 13:00 - 13:59 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

By the end of the session, attendees will gain a comprehensive understanding of the security mechanisms protecting mobile payment applications, the inherent vulnerabilities, and the sophisticated techniques employed by attackers to exploit these systems. This talk is designed to provide industry insights, maintaining a vendor-neutral perspective while focusing on the broader security landscape.

SpeakerBio: Adrian Garcia, Senior Security Expert at Adyen

Adrian Garcia serves as a Senior Security Expert at Adyen. With over ten years of experience in software security, Adrian specializes in mobile payment security, focusing on securing mobile products such as wallets and mobile points of sale. Passionate about reverse engineering, Adrian brings extensive knowledge of cryptography and payment security standards to his work.

Return to Index - Add to Google - ics Calendar file

Title: Breaking the Beam: Exploiting VSAT Satellite Modems from the Earth's Surface
When: Saturday, Aug 10, 16:30 - 17:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

VSAT satellite communication systems are widely used to provide two-way data and voice communications to remote areas, including maritime environments, crisis regions, and other locations where terrestrial communication infrastructure is limited or unavailable. In this presentation, we report on our security findings from our reverse-engineering efforts to exploit VSAT satellite modems from the Earth. We will focus on the Newtec MDM2200 from iDirect as an example. First, we explain how we reverse-engineered the software stack running on the modem device to find 0-day vulnerabilities. Then, we show how we reverse-engineered the network stack to devise attacks that can be launched by injecting wireless signals through the antenna dish of a VSAT terminal. Finally, we demonstrate our software-defined radio end-to-end attacks to inject bogus firmware updates and to gain a remote root shell access on the modem. To the best of knowledge, this represents the first successful demonstration of signal injection attacks on VSAT modems using software-defined radios from the Earth, while previous attacks on VSAT systems such as the ViaSat hack in 2022 were based on exploiting the operator's network through Internet VPN connections. Our work therefore enlarges significantly the attack surface of VSAT systems.

Our presentation at DEF CON is part of a project that has three parts.

In the first part, we focus on the inherent security issues in current VSAT system practices. This work will be appear in May at ACM WiSec 2024.

VSAsTer: Uncovering Inherent Security Issues in Current VSAT System Practices, Johannes Willbold, Moritz Schloegel, Robin Bisping, Martin Strohmeier, Thorsten Holz, Vincent Lenders, 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Seoul, Korea, May 2024.

The second part deals with the systematic evaluation of wireless signal injection attacks using a software-defined radio. This work will appear in August at Usenix Security 2024:

Wireless Signal Injection Attacks on VSAT Satellite Modems, Robin Bisping, Johannes Willbold, Martin Strohmeier, and Vincent Lenders, 33rd USENIX Security Symposium (USENIX Security), Philadelphia PA, USA, August 2024.

The third part of the project deals with reverse-engineering of the software and network stack of satellite modems and the development of exploits that can be injected over the air through the antenna dish of a VSAT terminal from the ground. This part shall be presented at DEF CON this year.

Speakers: Vincent Lenders,Johannes Willbold,Robin Bisping

SpeakerBio: Vincent Lenders, Cybersecurity Researcher and Head at Cyber-Defence Campus

Vincent Lenders is a cybersecurity researcher from Switzerland where he acts as the Head of the Cyber-Defence Campus. He has a Master and PhD degree from ETH Zurich in electrical engineering. He has over 15 years of practical experience in cybersecurity with a strong focus on the security of wireless networks. He is the co-founder of the OpenSky Network and has published over 150 scientific papers and two books, and presents regularly at cybersecurity conferences including Usenix Secuirty, DEFCON, IEEE S&P, NDSS, ACM CCS.

SpeakerBio: Johannes Willbold, PhD Student at Ruhr University Bochum

Johannes Willbold is a PhD student at the Ruhr University Bochum and researches the software security of space and satellite systems. In 2023, he published at the IEEE S&P, and presented on venues, including Black Hat US, REcon and TyphoonCon.

He organizes the yearly SpaceSec workshop (co-located with NDSS) and participated in the Hack-a-Sat 2 & 4 finals.

SpeakerBio: Robin Bisping, Security Engineer at Cyber-Defence Campus

Robin Bisping is a security engineer and former student of ETH Zurich and the Cyber-Defence Campus, where his research focused on the security of wireless networks and satellite communication systems.

Return to Index - Add to Google - ics Calendar file

VMV - Friday - 15:30-16:15 PDT

Title: Breaking Through Election Myths
When: Friday, Aug 9, 15:30 - 16:15 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

This talk will cover common voting machine myths and dispel common voting machine cases and fallacies that are prevalent in the media during election cycles and disinformation from social media and ‘experts’ from the perspective of a CIA HUMINT/Technical Officer now in the Cybersecurity field investigating corporate espionage and intentional sabotage. I will show- with pictures and evidence from previous Voting Machine Village work- that the sensational news headlines are not related to the reality of digital voting.

SpeakerBio: Will Baggett

Will Baggett is a Lead Investigator for Digital Forensics and Insider Threat at a Fiscal Infrastructure organization. He is also Director of Digital Forensics at Operation Safe Escape (volunteer role), a non-profit organization providing assistance to victims of domestic abuse. Will draws from his experience as a former CIA officer specializing in Technical and HUMINT Operations as well as a NATO SOF Cyber Security SME. He has extensive experience in the voting machine security effort and works to mitigate misinformation in this space with digital forensic analysis and facts.

Return to Index - Add to Google - ics Calendar file

Title: Bricked & Abandoned: How To Keep The IoT From Becoming An Internet of Trash
When: Friday, Aug 9, 17:00 - 17:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

In a world where technology and software are intertwined with our daily lives more than ever, a silent threat grows in the shadows.

End-of-life devices—abandoned by manufacturers - power our homes, hospitals, businesses and critical infrastructure. From the depths of the cyber underground, malicious software from cybercriminal and nation-state actors is seizing these forgotten devices and conscripting them into botnets and other malicious infrastructure.

For example, Black Lotus Labs revealed a chilling trend: 40,000 small office home office (SOHO) routers compromised and enrolled in the sinister 'Faceless' botnet - now powered by devices you own and thought were safe.

And it's not just routers. Critical medical devices, essential security hardware—smart home appliances. No gadget is safe. And, with the Internet of Things set to double in the next decade, billions of vulnerable devices marketed and sold to connect us risk robbing, dividing and defeating us in the years to come: a process one expert has termed “enshittification.”

After years of warnings from the cybersecurity community, alarms are finally sounding in the halls of power. But more is needed: a clarion call to reset, to redefine ownership and security in an age of smart, connected devices before it's too late.

In this panel you’ll be enlisted to join the fight. You’ll hear from experts working at the forefront of a fight to challenge the status quo and seek solutions to safeguard our digital futures.Are you ready to stand up for your right to a secure, connected world? The battle for control, for transparency- for a sustainable and resilient digital future begins now!

Speakers: Paul Roberts,Chris Wysopal,Cory Doctorow,Tarah Wheeler,Dennis Giese

SpeakerBio: Paul Roberts, Publisher and Editor in Chief at The Security Ledger

Paul Roberts is the publisher and Editor in Chief of The Security Ledger and the founder of Secure Repairs (securepairs.org) a coalition of cybersecurity and IT pros who support the right to repair.

SpeakerBio: Chris Wysopal, CTO at Veracode

Chris Wysopal is the CTO of Veracode, a provider of application security testing technology. Chris began his career as a vulnerability researcher at the renowned hacker think tank, L0pht. In 1998, Chris and 6 of his L0pht colleagues testified before the U.S. Senate on matters of U.S. government cybersecurity.

SpeakerBio: Cory Doctorow, Author

Cory Doctorow is a science fiction author, activist and journalist. He is the author of many books, most recently THE BEZZLE and THE LOST CAUSE. In 2020, he was inducted into the Canadian Science Fiction and Fantasy Hall of Fame.

SpeakerBio: Tarah Wheeler, Senior Fellow in Global Cyber Policy at Council on Foreign Relations

Tarah Wheeler is the founder and CEO of Red Queen Dynamics; a Senior Fellow in Global Cyber Policy at the Council on Foreign Relations; and a well-known speaker and writer on topics that include cyberwarfare, security best practices, future trends and more.

SpeakerBio: Dennis Giese

Dennis Giese is a researcher with the focus on the security and privacy of IoT devices. While being interested in physical security and lockpicking, he enjoys applied research and reverse engineering malware and all kinds of devices. His most known projects are the documentation and hacking of various vacuum robots. He calls himself a "robot collector" and his current vacuum robot army consists of over 60 different models from various vendors. He talked about his research at the Chaos Communication Congress, REcon BRX, NULLCON, and DEFCON.

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Bricks in the Air
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Bricks in the Air is a hands-on demo to teach the basics of low level protocols seen in aviation. The demo uses the I2C protocol and does not reveal actual security vulnerabilities in avionics or other systems in aviation.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Bricks in the Air
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Bricks in the Air is a hands-on demo to teach the basics of low level protocols seen in aviation. The demo uses the I2C protocol and does not reveal actual security vulnerabilities in avionics or other systems in aviation.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Bricks in the Air
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Bricks in the Air is a hands-on demo to teach the basics of low level protocols seen in aviation. The demo uses the I2C protocol and does not reveal actual security vulnerabilities in avionics or other systems in aviation.

Return to Index - Add to Google - ics Calendar file

BHV - Saturday - 10:00-10:59 PDT

Title: Bridging Space and Medicine
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

In the vast expanse of space, holographic teleportation—a futuristic blend of holography and teleportation—has revolutionized astronaut communication. Imagine beaming a lifelike 3D image of yourself across light-years. Now, consider its potential in medicine: remote surgeries, expert consultations, and training—where distance dissolves, and expertise transcends borders. Buckle up; holoconnect is our cosmic ticket to healing!

SpeakerBio: Fernando De La Peña Llaca, Aexa Aerospace

For 28 years, Fernando De La Peña Llaca has steered Aexa Aerospace with unwavering leadership. His passion for space exploration, combined with Aexa's cutting-edge expertise, has propelled the company to remarkable heights. Here's how his visionary leadership transformed Aexa into a Federal Contractor for prestigious entities:

1. NASA Collaboration:
    - Aexa's journey began with a shared vision for space. Fernando's commitment to NASA's mission led to strategic partnerships.
    - As an undergraduate, he patented a groundbreaking spacecraft engine fueled by anti-matter—an innovation that caught NASA's attention.
2. Defense and Industry Giants:
    - Aexa's portfolio expanded to include the US Department of Defense. Fernando's leadership secured contracts with industry titans:
    - Lockheed Martin: Collaborating on cutting-edge aerospace projects.
    - Aerojet Rocketdyne: Advancing propulsion technologies.
    - Teledyne Brown, KBR, and Thales Defense: Key partners in space exploration.
3. Influential Roles:
    - As former President of the National Contract Management Association (NCMA) Space City Houston chapter at NASA JSC, Fernando shaped contract management practices.
    - His chairmanship of the Johnson Space Center Small Business Council fostered collaboration and growth.
4. Community Engagement:
    - Fernando's impact extends beyond contracts. He serves on the Bay Area Houston Economic Partnership Board of Directors (BAHEP), driving regional space initiatives.
    - As aerospace liaison for the Clear Lake Chamber of Commerce, he bridges industry and community interests.
5. Defense Industrial Base Leadership:
    - Fernando's role as Chief of the Infragard Defense Industrial Base SIG underscores his commitment to national security.
    - The Defense Industrial Base Sector, vital for military readiness, benefits from his expertise.
6. Awards and Recognition:
    - The Small Business Champion of the Year Award from the Small Business Administration celebrates his impact.
    - NASA's Innovation of the Year Group Award 2022 further validates Aexa's contributions.

Fernando De La Peña Llaca's legacy is etched in the stars—a testament to visionary leadership and unwavering dedication to space exploration.

Return to Index - Add to Google - ics Calendar file

AIV - Saturday - 15:00-15:59 PDT

Title: Bridging the Experience Gap in Machine Learning Security
When: Saturday, Aug 10, 15:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

This panel will explore the critical challenges and opportunities in developing a robust workforce for AI and machine learning (ML) security. As AI systems become increasingly prevalent across industries, the need for skilled professionals who can safeguard these technologies against adversarial attacks and vulnerabilities has never been greater.

A key focus of the discussion will be addressing the significant shortage of practitioners with hands-on experience in securing ML models deployed in real-world adversarial environments. Panelists will examine how this lack of battle-tested expertise impacts the industry's ability to defend against sophisticated attacks and discuss strategies for cultivating this essential skill set.

Speakers: Kellee Wicker (Moderator),Christine Lai,David Lo,Austin Carson,Nick Landers

SpeakerBio: Kellee Wicker (Moderator), The Wilson Center
No BIO available
SpeakerBio: Christine Lai, Cybersecurity Research Specialist at DHS Cyber Security and Infrastructure Security Agency

Christine Lai is a cybersecurity research specialist in the Office of the Technical Director at the Cybersecurity and Infrastructure Security Agency (CISA), where she currently serves as the AI Security lead for the agency. Prior to joining CISA, she was a cybersecurity and machine learning researcher on critical infrastructure programs at Sandia National Laboratories in Albuquerque, NM.

SpeakerBio: David Lo, SMU
No BIO available
SpeakerBio: Austin Carson, Seed AI
No BIO available
SpeakerBio: Nick Landers, Dreadnode
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 12:00-12:45 PDT

Title: Bridging the Gap: How the American Legion Provides Veterans with a Sense of Belonging and Support
When: Friday, Aug 9, 12:00 - 12:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:
SpeakerBio: Chris Davis
No BIO available

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 14:05-14:50 PDT

Title: Brief History of GRC
When: Saturday, Aug 10, 14:05 - 14:50 PDT
Where: Virtual

Description:
SpeakerBio: Allen Baranov

World's only AAA-rated GRC hacker. DEFCON Group 11613 (Melbourne) founder. Time Magazine's Person of the year in 2006. Infinidash expert

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 13:30-14:15 PDT

Title: Bringing Down North Korea
When: Sunday, Aug 11, 13:30 - 14:15 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

In January 2021, I discovered that North Korean state-backed agents were targeting security researchers. A few people got hit, including me. They didn't get anything, but I was very frustrated by the inaction of law enforcement, intelligence agencies, and DoD. I decided I was going to see what I could do. Armed with my computer and a bunch of Takis I got to work mapping out NK's infrastructure. This talk will detail the methods and tools I used to bring down North Korea's internet for 9 days along with the architectural and other vulnerabilities I found that allowed for the attack. This presentation will cover the technical aspects of the attack, criticisms of the DoD and Intel Community, praise from the DoD and Intel Community and the implications of a small team of hackers, or just one dude, causing real-world impact. Attendees will gain insights into create methodologies for network exploitation and the ethical, practical, and resistance from the government to cyber guerrilla warfare, demonstrating the need for agile and responsive cyber capabilities in the modern world.

1. Greenberg, Andy. "The Hacker Who Took Down North Korea's Internet." Wired. link.
2. Greenberg, Andy. "North Korea Hacker Internet Outage." Wired. link.
3. DEF CON 21 Talk: "Conducting massive attacks with open source distributed computing" link
4. DEF CON 29 Talk: "WTF happened to that tool that was like Shodan but for web app vulns?" link
5. DEF CON 21 Talk: "The Dawn of Web 3.0: Website Mapping and Vulnerability Scanning" link.
6. The Register: link

SpeakerBio: Alejandro Caceres, Owner at Hyperion Gray

Alex is the dude that took down North Korea's Internet routing for 9 days. He owns Hyperion Gray and creates a bunch of open source software.

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 14:30-15:30 PDT

Title: BTV Conversations: Exploring the Cyberpsychology of Cyber Defender Acceptance Behaviors and Personality Traits
When: Friday, Aug 9, 14:30 - 15:30 PDT
Where: LVCC West/Floor 3/W311-W313 - Map

Description:

BTV Conversations explores creative, personal, or cutting-edge Blue Team topics in an interactive, conversational format.

Todd Fletcher will introduce listeners to the topic of cyberpsychology. This discussion investigates the psychological and ethical dimensions influencing cybersecurity practitioners' behaviors towards cyber defense, utilizing Q-Methodology to elucidate diverse motivations and ethical perspectives within the community. The connected study involves participants sorting statements reflecting their views on cybersecurity, providing insights into common typologies and perspectives. Findings aim to inform nuanced cybersecurity strategies that prioritize both security and practitioners' mental well-being, adhering to strict ethical standards. This research contributes significantly to Cyberpsychology, enhancing understanding and practical approaches to contemporary cybersecurity challenges.

SpeakerBio: Todd Fletcher, Principal Consultant at CrowdStrike

With over 25 years of experience in IT leadership, network, application, and security engineering, I am a Principal Consultant at CrowdStrike, a leading provider of cloud-native endpoint and workload protection solutions. I hold a Master of Science in Cybersecurity and Information Assurance, and a Certified Information Systems Security Professional (CISSP) credential.

As a consultant, I assist information security teams from various sectors to assess their security posture, and develop plans to close security gaps while achieving technical and executive success. I am skilled in agile project management, systems automation, SIEM, SOAR, penetration tools, and security program development based on the NIST and other frameworks. I have also conducted cloud security and automation with Azure DevSecOps.

Besides my consulting role, I am pursuing a PhD in cyberpsychology at Birmingham City University, where I explore the psychological aspects of cybersecurity, such as user behavior, motivation, trust, and risk perception. I am passionate about pushing the boundaries of how to drive successful security initiatives from both a technical and psychological perspective with organizations across many industries.

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 15:30-16:30 PDT

Title: BTV Conversations: Touch Grass to Combat Burnout
When: Friday, Aug 9, 15:30 - 16:30 PDT
Where: LVCC West/Floor 3/W311-W313 - Map

Description:

BTV Conversations explores creative, personal, or cutting-edge Blue Team topics in an interactive, conversational format.

CtrlAltFu will share personal experiences combatting work stress and burnout through physical activity, and invite a conversation about others' experiences and strategies to combat burnout.

SpeakerBio: CtrlAltFu
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Building a Cyber Threat Intelligence Program from scratch for free!
When: Friday, Aug 9, 10:00 - 11:30 PDT
Where: LVCC West/Floor 3/W309 - Map

Description:

Outline:
Intro to CTI
- What is CTI
- Threat Intel Types
- Why build a CTI

Major components for a CTI program - Data Collection/Feeds - Parsing and Storage - Enrichment - Dissemination

Steps in building CTI program - Technology - People - Process

Lab: Step-by-step walkthrough of two CTI platforms (MISP and OpenCTI) - Install the CTI platforms - Add relevant data sources - Analyzing data sources - Effective data correlation

Metrics to track the progress and success of a CTI program Maturity Model of a CTI program

Are you eager to understand your threat actors, targets, and behaviors? Are you constrained by resources to get a cyber threat intel program up and running? Are you not sure which tools to start with for cyber threat intel? If so, then this workshop is for you! We walkthrough how you can build a cyber threat intelligence program using open-source tools at minimum cost. We discuss the major components of a cyber threat intel program and the steps (including people, process, and technology) to bring your program to existence. In this workshop, we will show you how to set up and install open-source threat intelligence tools and relevant feeds. We also demonstrate how to analyze and correlate data to produce actionable intelligence. Finally, we discuss metrics and a maturity model for your program.

Speakers: Apurv Singh Gautam,Karan Dwivedi

SpeakerBio: Apurv Singh Gautam, Cybercrime Researcher at Cyble

Apurv Singh Gautam is a Cybercrime Researcher working at Cyble. He focuses on monitoring and analyzing a wide spectrum of sources by utilizing HUMINT, SOCMINT, and OSINT and producing finished threat intelligence. Apurv has contributed to the SANS FOR589 course on Cybercrime Intelligence. He is passionate about giving back to the community and has already delivered several national and international talks and seminars at conferences like the SANS OSINT Summit, Defcon Blue Team Village, BSides Singapore, local security meetups, schools, and colleges. He loves volunteering with Station X to help students navigate into Cybersecurity. He looks forward to the end of the day to play and stream one of the AAA games, Rainbow Six Siege.

SpeakerBio: Karan Dwivedi

Karan Dwivedi is a recognized cybersecurity expert. Currently, he serves as a security engineering manager at Google. Karan has led large-scale security projects at Google and Yahoo in the US for products like Google Search, Google Assistant, Yahoo Mail, Yahoo Finance, Flickr, etc, to safeguard over a billion users. At Yahoo, he was part of the security team responding to the world's largest data breach. Karan contributed to the latest internet standard for scoring vulnerabilities, the Common Vulnerability Scoring System (CVSS 4.0). He is featured in major media like Hakin9 Media Magazine, Forensic Focus News, etc. He has delivered talks at national and international conferences like Tech Ex North America, Tech Summit SF, BSides Las Vegas, National Cyber Summit, etc, to influence private and public sectors. Karan was featured as a subject matter expert in the Google Cybersecurity Certificate program launched in May 2023 on Coursera, which had an enrollment of over 41000 students in a few weeks.

ICSV - Sunday - 12:00-12:59 PDT

Title: Building a foundation with the 5 critical controls
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:
SpeakerBio: Dillon Lee

Generic cyber guy in polo

Return to Index - Add to Google - ics Calendar file

CHV - Friday - 13:30-13:59 PDT

Title: Building a secure and resilient nationwide EV charging network: the role of hackers in the clean energy revolution
When: Friday, Aug 9, 13:30 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Unprecedented investments in vehicle electrification are creating new pathways for hackers to exploit EVs and EV chargers. Many of these risks are theoretical and have not been demonstrated in the wild…yet. Policymakers are racing to better understand systemic cyber risks present in this new EV ecosystem—particularly those which might impact the electric grid—so we can devise effective mitigations now. This talk offers a White House policymaker's perspective on the changing EV landscape, new policy measures under consideration to identify and reduce the impact of vulnerabilities, and the critical role that hackers can play in focusing our work.

Speakers: Harry Krejsa,Sarah Hipel

SpeakerBio: Harry Krejsa, Assistant National Cyber Director for Strategy at ONCD

Harry Krejsa is the Assistant National Cyber Director for Strategy. He leads the office's development of cyber and technology strategy for domestic and international policy, including co-directing the drafting, interagency approval, and rollout of President Joe Biden's National Cybersecurity Strategy. Prior to joining the Office of the National Cyber Director, Harry oversaw strategy and U.S.-China competition for the Department of Defense's cyber policy office. He drafted the 2018 DoD Cyber Strategy and inaugural Cyber Posture Review, which provided guidance for using new offensive military authorities to deter and disrupt adversary cyber campaigns, and negotiated numerous "Hunt Forward" joint operations with foreign militaries to root out adversary malware on strategic systems. Upon leaving DoD he was awarded the Office of the Secretary of Defense Medal for Exceptional Public Service. From 2019-2020 Harry was detailed to serve as Director of the Integration Cell at the U.S. Cyberspace Solarium Commission, where he led research on emerging technology trends and their implications for U.S. government policy. He oversaw the Commission's strategy and policy development on norms and values in technology design, artificial intelligence, election cybersecurity, and China's influence over strategic technologies. Before joining government, Harry was a Fellow at the Center for a New American Security where he researched U.S.-China economic and technology competition, broader Indo-Pacific security strategy, and the intersection of foreign and domestic policy in the United States. Harry also worked as a professional staff member for the Congressional Joint Economic Committee, served as a researcher at the Center for the Study of Chinese Military Affairs at National Defense University, led field analysis on political transition in Myanmar, piloted anti-terror training programs in South Asia, and completed a Fulbright Fellowship in Taiwan. Harry's policy writings have appeared in Foreign Affairs, Politico, War on the Rocks, Fortune, and a number of regional American newspapers. His analysis has been featured in outlets like CBS News and Bloomberg, and he has given televised Chinese-language commentary to Voice of America. He is a Lecturer of International Affairs at George Washington University on defense and technology policy.

SpeakerBio: Sarah Hipel, Standards and Reliability Program Manager at ONCD
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Building Surgical Implants: A Comprehensive Guide to APT-style Techniques
When: Saturday, Aug 10, 13:00 - 13:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Explore the realm of crafting payloads with precision at DEFCON 32 in our session, "Mastering APT-Style Implants: 101." This deep dive experience goes beyond theory, providing practical insights into the development of payloads inspired by Advanced Persistent Threats (APTs).

Attendees will gain a holistic mindset by comprehending—an objective-based methodology for offensive cyber operations. Gain insights into real-world APT tactics and historical perspectives.

This is followed by practical payload development, AI integration, and comprehending industry-relevant tools, from line-by-line code to compiler settings necessary to ensure payload success. These techniques are then wrapped into stealth and operation security concepts with a scenario-based objective targeting a matured environment representative of today's real-world environments.

At the end of the deep dive, attendees will have experienced the payload development cycle from the perspective of a nation-state adversary. Comprehend the mindset necessary to operate in today's most mature environments and the practical knowledge to craft their implants.

SpeakerBio: John Rodriguez
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:30-12:30 PDT

Title: Building the Ultimate Budget-Friendly Low Earth Orbit Satellite Ground Station
When: Friday, Aug 9, 10:30 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

In this workshop, we explore the design, construction, and configuration of cost-effective Low Earth Orbit (LEO) satellite ground stations using open source tools. The aim is to demonstrate that high-quality ground stations can be developed on a limited budget without sacrificing performance. We will delve into the selection of hardware components, the integration process, and the software tools necessary for seamless operation. Additionally, real-world applications and case studies will be showcased to highlight the practical benefits and potential of these budget-friendly solutions. Attendees will leave with a comprehensive understanding of how to leverage open source resources to build and operate efficient ground stations, making advanced aerospace technology accessible to enthusiasts and professionals alike.

SpeakerBio: Victor Fernandez Minguillon

Victor is a Senior Red Team Analyst at United Airlines with 7 years of experience in offensive security. After immigrating to the United States in 2017 from Spain, he started his stateside career at Underwriter Laboratories doing penetration testing on medical device technologies, including software and hardware-embedded devices, wireless devices, and web and mobile applications. In his current position, he performs and manages Red Team Engagements, Attack Surface Reduction assessments, Physical Engagements, and handles United Airlines' Vulnerability Disclosure Program to help enhance United's cybersecurity posture. In his free time, he likes to spend time with his wife and three children (hackers are great at hide-and-seek).

Return to Index - Add to Google - ics Calendar file

Title: Building Your Red-Teaming Co-Pilot: Navigating the New Cyber Era with Pretrained Gen-AI
When: Friday, Aug 9, 16:00 - 16:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

Amid the Gen-AI revolution, notably through the rise of Large Language Models (LLMs), the cybersecurity landscape faces opportunities and challenges. These advanced AI models have successfully analyzed texts at unprecedented speeds, offering profound insights into vast data pools. However, this rapid technological growth has paved the way for sophisticated Gen-AI-powered cyber threats that exploit these systems' adaptable, polymorphic nature, outpacing traditional defenses.

This presentation seeks to empower red teamers by unveiling the potential of open-source Gen-AI as a formidable ally in cybersecurity. Focusing on practical application, we will guide participants through constructing their own Gen-AI-based "co-pilot," leveraging LLMs to enhance vulnerability identification and defense mechanisms.

Attendees will be introduced to the fundamentals of Gen-AI, including cost-effective strategies for fine-tuning LLMs using custom datasets drawn from pentest reports, bug bounties, and more. The discussion will extend to innovative, memory-efficient training methods such as LORA (Low-Rank Adaptation) and Quantized Low-Rank Adaptation (QLORA), making training an LLM on a modest single GPU setup feasible.

Designed for beginners with no prior AI experience, this talk aims to equip red teamers with powerful, open-source AI tools to accelerate vulnerability detection. By harnessing Gen-AI, cybersecurity professionals can stay one step ahead, identifying and mitigating potential threats at machine speed, ensuring they outpace adversaries in the ongoing cyber battle.

SpeakerBio: Gaspard Baye, AI Researcher & Ph.D. Candidate

Gaspard Baye, a PhD candidate in cyber-AI, brings over five years of industry experience, successfully leading teams to address over 100 critical challenges across 10 evaluations. His contributions include publishing six Cyber-AI algorithms, cited nearly 40 times in esteemed IEEE conferences and journals such as NeurIPS, PMLR, IEEE ISNCC, and IEEE/ACM MICRO'22. Recognized with a CVE for his cybersecurity work, Gaspard has fortified defenses for renowned firms like Nokia and Ford, earning places in multiple Hall of Fames.

Return to Index - Add to Google - ics Calendar file

Title: Building Zero Trust in ICS
When: Saturday, Aug 10, 15:30 - 15:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:
SpeakerBio: Sting

Sting(¡), Master of Software Engineering from Fudan University, previously worked for Siemens Group and Emerson Process Control. In the past few years, Sting has been focusing on penetration testing and security defense construction work in the ICS field. Attended 2018 Kcon Hacker Conference /2019 ISC Internet Security Conference /INSEC World Information Security Conference. Create an industrial control Security Red Team IRT(industrial Red Team) to industrial control security as the goal of the Red Team organization, from the technical direction and technical depth are based on industrial control security as the main line. Familiar with Siemens PLC, AB PLC, Schneider PLC, Hollysys DCS and Supper control DCS system. Sting has been developed ICS Windows, the first industrial penetration platform based on Windows system.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 13:00-14:59 PDT

Title: BYOS – Bring Your Own Satellite
When: Friday, Aug 9, 13:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

In this workshop, attendees are introduced to the basics of satellite communication in a hands-on manner. Also, through the power of virtualization and open-source software, attendees will get a step-by-step guide to create their own personal satellite lab, while helping discover the fundamental principles of satellite communication, from orbital mechanics to data transmission protocols, as you design, simulate, and experiment with satellite systems in a risk-free, virtual environment. Unveil the secrets of satellite technology, gain hands-on experience with real-world scenarios, and configuring and controlling your virtual satellite. This unique learning experience equips you with the knowledge and practical skills needed to explore the possibilities of satellite communication. Unlock the universe of opportunities that satellite communication offers, right from your own laptop.

Attendee Requirements: - A moder laptop with VMware Workstation or VMware Fusion Installed. - Both Intel/AMD64 and ARM64 are supported in this workshop - Internet Access is not Required but the ability to connect to a local Wi-Fi network will be in order to access the workshop materials.

Audience Skill Level: Beginner

BYOS is a beginner friendly workshop that does require some use of the Linux command line, however if you have never used the command line before, you can still be successful in this lab.

Some concepts will be new to attendees and the workshop is setup to allow ample time for questions and troubleshooting.

SpeakerBio: Tim Fowler

Tim Fowler is an Offensive Security Analyst with Black Hills Information Security and has over a decade of experience working in information security. He has worked for Fortune 100 financial institutions as well as a consultant, providing penetration testing and red team services. Tim is passionate about sharing his knowledge with others and has had the pleasure of speaking at multiple security conferences across the county. He is also the founder of the educational centric company ETHOS Labs, and the author of the Introduction to Cybersecurity in Space Systems course. When not hacking away as a clients' network or writing the subsequent report, researching cybersecurity in space, or developing functional CubeSats, Tim loves spending time with his wife and son and working in his workshop with his collection of hand tools and CNC machines.

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 17:00-17:59 PDT

Title: Bypass 101
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

There are loads of ways to get through a door without actually attacking the lock itself, including using the egress hardware, access control hardware, and countless other techniques to gain entry. Learn how to do these attacks in this talk!

SpeakerBio: Karen Ng, Risk Analyst at GGR Security

Karen is a Risk Analyst at GGR Security, and is one of GGR's entry team for physical penetration tests. She has a strong interest in physical security, delivering trainings on physical security vulnerabilities to a wide range of audiences. Karen comes from a background in engineering and has extensive experience in major event logistics. She is one of the Village Leads at the Physical Security Village, and works with the rest of the PSV team to teach how to recognize and fix security exploits to the community. Graphic design is her passion.

Return to Index - Add to Google - ics Calendar file

PSV - Sunday - 10:30-11:30 PDT

Title: Bypass 101
When: Sunday, Aug 11, 10:30 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

There are loads of ways to get through a door without actually attacking the lock itself, including using the egress hardware, access control hardware, and countless other techniques to gain entry. Learn how to do these attacks in this talk!

SpeakerBio: Karen Ng, Risk Analyst at GGR Security

Karen is a Risk Analyst at GGR Security, and is one of GGR's entry team for physical penetration tests. She has a strong interest in physical security, delivering trainings on physical security vulnerabilities to a wide range of audiences. Karen comes from a background in engineering and has extensive experience in major event logistics. She is one of the Village Leads at the Physical Security Village, and works with the rest of the PSV team to teach how to recognize and fix security exploits to the community. Graphic design is her passion.

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 13:00-13:59 PDT

Title: Bypass 101
When: Friday, Aug 9, 13:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

There are loads of ways to get through a door without actually attacking the lock itself, including using the egress hardware, access control hardware, and countless other techniques to gain entry. Learn how to do these attacks in this talk!

Speakers: Karen Ng,Sam Mayers

SpeakerBio: Karen Ng, Risk Analyst at GGR Security

Karen is a Risk Analyst at GGR Security, and is one of GGR's entry team for physical penetration tests. She has a strong interest in physical security, delivering trainings on physical security vulnerabilities to a wide range of audiences. Karen comes from a background in engineering and has extensive experience in major event logistics. She is one of the Village Leads at the Physical Security Village, and works with the rest of the PSV team to teach how to recognize and fix security exploits to the community. Graphic design is her passion.

SpeakerBio: Sam Mayers, Security Researcher at Beazley Security

Sam is a Security Researcher at Beazley Security with a focus on threat intelligence and cybercrime. She is a board member for non-profits such as Physical Security Village and clearsear.ch. Within Physical Security Village she focuses on discovering and teaching new physical security issues to members and attendees during village events.

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 15:00-15:30 PDT

Title: Bypass 102
When: Saturday, Aug 10, 15:00 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Now that you're familiar with the techniques used to bypass locks in some door installation, come and learn the remediations for these common bypasses. In this talk, you will learn how to protect against or harden against attacks such as the Under the Door attack, latch slipping, and more.

Speakers:Karen Ng,Terry Luan

SpeakerBio: Karen Ng, Risk Analyst at GGR Security

Karen is a Risk Analyst at GGR Security, and is one of GGR's entry team for physical penetration tests. She has a strong interest in physical security, delivering trainings on physical security vulnerabilities to a wide range of audiences. Karen comes from a background in engineering and has extensive experience in major event logistics. She is one of the Village Leads at the Physical Security Village, and works with the rest of the PSV team to teach how to recognize and fix security exploits to the community. Graphic design is her passion.

SpeakerBio: Terry Luan

Terry is a recent Computer Engineering graduate. As one of the Village Leads for the Physical Security Village, he helps with much of the Village logistics, as well as volunteer and external management. His main areas of interest are in security (both physical and virtual) and lockpicking, and he loves teaching people about various security exploits.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 12:00-12:50 PDT

Title: Bypassing Corporate controls on Mac Devices
When: Friday, Aug 9, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

With widespread zero trust security adoption there has also been more focus put into corporate controls. As a red teamer what this means is that bypassing EDR is not enough, you also need to think about application allowlisting, DLP solutions, Managed browsers, MDM profiles and custom DnR tooling. In this talk I will walkthrough Mac capabilities that corporate controls leverage, their limitations and features to build into your payload and payload delivery to circumvent these restrictions.

Speakers: Adwiteeya Agrawal,Ian Foster

SpeakerBio: Adwiteeya Agrawal
No BIO available
SpeakerBio: Ian Foster
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 12:05-12:40 PDT

Title: Bypassing WHOIS Rate Limiting and Alerting on Fresh Enterprise Domains
When: Friday, Aug 9, 12:05 - 12:40 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

WHOIS data is a prime resources for identifying apex domains owned by a company. Unfortunately that data is typically locked up behind rate limited systems, third party APIs, or expensive bulk purchases. We developed whoiswatcher to run in serverless cloud (where we have clocked it at 1-1.5MM domains per day) or by using IPv6 proxying (can hit 150-200k domains per day with a small VPC). This makes it a perfect candidate to build a WHOIS dataset, review historic WHOIS records, and alert you on fresh enterprise domains. We will demo all this and more!

SpeakerBio: Willis Vandevanter
No BIO available

Return to Index - Add to Google - ics Calendar file

DL - Friday - 12:00-13:45 PDT

Title: BypassIT - Using AutoIT & Similar Tools for Covert Payload Delivery
When: Friday, Aug 9, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W304 - Map

Description:

BypassIT is a framework for covert delivery of malware, using AutoIT, AutoHotKey, and other Live off the Land (LotL) tools to deliver payloads and avoid detection. These techniques were derived from reversing attacks observed in the wild by DarkGate and other MaaS actors, revealing universal principles and methods useful for red teaming or internal testing. The framework will consist of a series of tools, techniques, and methods along with testing and reporting on effectiveness, as it relates to evading multiple specific antivirus products.

Speakers: Ezra Woods,Mike Manrod

SpeakerBio: Ezra Woods, Information Security Analyst, Department of Economic Security at Arizona

Ezra Woods is a recent cybersecurity graduate from Grand Canyon University, working as an Information Security Analyst for Arizona's Department of Economic Security. Captain of Grand Canyon University's collegiate cyber defense team, and Team Lead for the Arizona Cyber Threat Response Alliance's Threat Intelligence Support Unit (TISU).

SpeakerBio: Mike Manrod, Chief Information Security Officer at Grand Canyon Education

Mike serves as the Chief Information Security Officer for Grand Canyon Education, responsible for leading the security team and formulating the vision and strategy for protecting students, staff, and information assets across the enterprise. He also serves as Adjunct Faculty for Grand Canyon University, teaching Malware Analysis and Threat Intelligence. Previous experiences include serving as a threat prevention engineer for Check Point and working as a consultant and analyst for other organizations.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 15:00-17:59 PDT

Title: C2Society / DC702 Intro to CTFs
When: Friday, Aug 9, 15:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Breaking into the capture the flag (CTF) world can be daunting and many people are overwhelmed when faced with participation in these events and challenges. With how beneficial the various challenges can be to both beginners and seasoned professionals, we want to demystify this world and help people get the most out of them. This is a full hands-on course on how to do CTFs, tools and more. Bring your laptops!

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 10:00-10:59 PDT

Title: Caido Internals Deep-Dive
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

Get a deep-dive into the more complex and powerful parts of Caido by its creators. We will cover various topics ranging from: - Using HttpQL at its full potential - Creating complex workflows and leveraging them in your day-to-day - Using the Caido GraphQL API to extend the tool - Building frontend plugins - And more!

We will also be there to answer all your complex technical questions.

Pre-Requisites: - Install Caido if you want to follow along.

SpeakerBio: Emile Fugulin, Caido

Emile was a freelance DevOps & backend developer for many years prior to starting Caido. He always had a passion for security, and working on Caido is the perfect combination of both!

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 21:00-01:59 PDT

Title: Capitol Technology University (CTU)
When: Friday, Aug 9, 21:00 - 01:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Join Capitol Technology University for a night of fun, drinks, and networking amongst like-minded peers! Capitol Tech's industry-expert leadership will be discussing exciting career paths in cybersecurity, as well as the future of cyber higher education.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Capture the Packet
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

This event was born out of the fires of DEF CON. Through years of analyzing network traffic for the Wall of Sheep and teaching others how to do the same, we built this system as a way to help the growing numbers in our community learn (fast). Then it quickly turned into the first defensive based CTF at DEF CON and is one of the longer running competitions at con with a twist... Each year we practically re-invent ourselves, bringing the latest tools & techniques along with never seen before content across 17 categories to unleash hell on the mostly-unsuspecting attendees. For ’24 we have added tons of new content, and new types of challenges never seen before.

Come compete in the world's most challenging cyber defense competition based on the Aries Security Cyber Range. Tear through the challenges, traverse a hostile enterprise class network, and diligently analyze what is found in order to make it out unscathed. Not only glory, but prizes await those that emerge victorious from this upgraded labyrinth, so only the best prepared and battle hardened will escape the crucible.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Capture the Packet
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

This event was born out of the fires of DEF CON. Through years of analyzing network traffic for the Wall of Sheep and teaching others how to do the same, we built this system as a way to help the growing numbers in our community learn (fast). Then it quickly turned into the first defensive based CTF at DEF CON and is one of the longer running competitions at con with a twist... Each year we practically re-invent ourselves, bringing the latest tools & techniques along with never seen before content across 17 categories to unleash hell on the mostly-unsuspecting attendees. For ’24 we have added tons of new content, and new types of challenges never seen before.

Come compete in the world's most challenging cyber defense competition based on the Aries Security Cyber Range. Tear through the challenges, traverse a hostile enterprise class network, and diligently analyze what is found in order to make it out unscathed. Not only glory, but prizes await those that emerge victorious from this upgraded labyrinth, so only the best prepared and battle hardened will escape the crucible.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Capture the Packet
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

This event was born out of the fires of DEF CON. Through years of analyzing network traffic for the Wall of Sheep and teaching others how to do the same, we built this system as a way to help the growing numbers in our community learn (fast). Then it quickly turned into the first defensive based CTF at DEF CON and is one of the longer running competitions at con with a twist... Each year we practically re-invent ourselves, bringing the latest tools & techniques along with never seen before content across 17 categories to unleash hell on the mostly-unsuspecting attendees. For ’24 we have added tons of new content, and new types of challenges never seen before.

Come compete in the world's most challenging cyber defense competition based on the Aries Security Cyber Range. Tear through the challenges, traverse a hostile enterprise class network, and diligently analyze what is found in order to make it out unscathed. Not only glory, but prizes await those that emerge victorious from this upgraded labyrinth, so only the best prepared and battle hardened will escape the crucible.

Return to Index - Add to Google - ics Calendar file

CHV - Friday - 10:00-17:59 PDT

Title: Car Hacking Village Activities
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map

Description:

CHV 101

This booth will have several reverse engineer demonstrations and an automotive threat intelligence review.

- Reverse Engineering Demonstration(s)
- Live vehicle communications via remote controls
- EV-based Hardware-in-the-Loop (HIL) demonstrations
- Automotive Threat Intelligence
- How to gather threat intelligence related to the automotive industry
- What the current threat landscape looks like today

CHV CTF

There will be 10-15 automotive security CTF challenges this year ranging from reverse engineering, telemetry, grand theft auto, crypto, vehicle networks, and exploitation.

1st place prize is a car!

CHV Kids

A fun scavenger hunt designed for DCNextGen kids to participate in and learn about the Car Hacking Village.

There will be swag items handed out to the kids as they move through the scavenger hunt.

CHV Mechanics

There will be 1 Semi-Truck and 2 Electric Vehicles on site for people to plug into.

DEFCON attendees must follow the rules for each of the vehicles. There will be large ORANGE signs with the rules detailed on them.

Return to Index - Add to Google - ics Calendar file

CHV - Saturday - 10:00-17:59 PDT

Title: Car Hacking Village Activities
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map

Description:

CHV 101

This booth will have several reverse engineer demonstrations and an automotive threat intelligence review.

- Reverse Engineering Demonstration(s)
- Live vehicle communications via remote controls
- EV-based Hardware-in-the-Loop (HIL) demonstrations
- Automotive Threat Intelligence
- How to gather threat intelligence related to the automotive industry
- What the current threat landscape looks like today

CHV CTF

There will be 10-15 automotive security CTF challenges this year ranging from reverse engineering, telemetry, grand theft auto, crypto, vehicle networks, and exploitation.

1st place prize is a car!

CHV Kids

A fun scavenger hunt designed for DCNextGen kids to participate in and learn about the Car Hacking Village.

There will be swag items handed out to the kids as they move through the scavenger hunt.

CHV Mechanics

There will be 1 Semi-Truck and 2 Electric Vehicles on site for people to plug into.

DEFCON attendees must follow the rules for each of the vehicles. There will be large ORANGE signs with the rules detailed on them.

Return to Index - Add to Google - ics Calendar file

CHV - Sunday - 10:00-12:59 PDT

Title: Car Hacking Village Activities
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map

Description:

CHV 101

This booth will have several reverse engineer demonstrations and an automotive threat intelligence review.

- Reverse Engineering Demonstration(s)
- Live vehicle communications via remote controls
- EV-based Hardware-in-the-Loop (HIL) demonstrations
- Automotive Threat Intelligence
- How to gather threat intelligence related to the automotive industry
- What the current threat landscape looks like today

CHV CTF

There will be 10-15 automotive security CTF challenges this year ranging from reverse engineering, telemetry, grand theft auto, crypto, vehicle networks, and exploitation.

1st place prize is a car!

CHV Kids

A fun scavenger hunt designed for DCNextGen kids to participate in and learn about the Car Hacking Village.

There will be swag items handed out to the kids as they move through the scavenger hunt.

CHV Mechanics

There will be 1 Semi-Truck and 2 Electric Vehicles on site for people to plug into.

DEFCON attendees must follow the rules for each of the vehicles. There will be large ORANGE signs with the rules detailed on them.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-16:30 PDT

Title: Car Hacking Village CTF
When: Friday, Aug 9, 10:00 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map

Description:

The Car Hacking Village CTF is a fun interactive challenge which gives contestants first hand experience to interact with automotive technologies. We work with multiple automotive OEMs and suppliers to ensure our challenges give a real-world experience to car hacking. We understand hacking cars can be expensive, so please come check out our village and flex your skills in hacking automotive technologies.

With the largest collection of hackers in one area, there's no better way to understand the security state of an industry without bringing it to security professionals to break. Over the past 10 years, the Car Hacking Village has been the focal point of interest for new hackers entering the automotive industry to learn, be a part of and actually test out automotive technologies. We plan to use this event to keep drawing attention to the automotive security industry through hands-on challenges.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Car Hacking Village CTF
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map

Description:

The Car Hacking Village CTF is a fun interactive challenge which gives contestants first hand experience to interact with automotive technologies. We work with multiple automotive OEMs and suppliers to ensure our challenges give a real-world experience to car hacking. We understand hacking cars can be expensive, so please come check out our village and flex your skills in hacking automotive technologies.

With the largest collection of hackers in one area, there's no better way to understand the security state of an industry without bringing it to security professionals to break. Over the past 10 years, the Car Hacking Village has been the focal point of interest for new hackers entering the automotive industry to learn, be a part of and actually test out automotive technologies. We plan to use this event to keep drawing attention to the automotive security industry through hands-on challenges.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Car Hacking Village CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-01 - Map

Description:

The Car Hacking Village CTF is a fun interactive challenge which gives contestants first hand experience to interact with automotive technologies. We work with multiple automotive OEMs and suppliers to ensure our challenges give a real-world experience to car hacking. We understand hacking cars can be expensive, so please come check out our village and flex your skills in hacking automotive technologies.

With the largest collection of hackers in one area, there's no better way to understand the security state of an industry without bringing it to security professionals to break. Over the past 10 years, the Car Hacking Village has been the focal point of interest for new hackers entering the automotive industry to learn, be a part of and actually test out automotive technologies. We plan to use this event to keep drawing attention to the automotive security industry through hands-on challenges.

Return to Index - Add to Google - ics Calendar file

ICSV - Sunday - 13:00-13:25 PDT

Title: Career Development - The Human Element
When: Sunday, Aug 11, 13:00 - 13:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:
SpeakerBio: Kirsten Renner, VP of Talent at SilverEdge Gov Solutions

Serial community volunteer and recruiting expert

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-10:30 PDT

Title: Case Study: Hacking Smart Lock For Fun and Profit
When: Saturday, Aug 10, 10:00 - 10:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Caso de estudio sobre como se realizo el pentest de una Chapa inteligente que se pretendía utilizar en la Fascia de cajeros automáticos, al final, se logro encontrar una vulnerabilidad que ponía en riesgo la apertura de cualquier chapa perteneciente a la empresa fabricante, ya que las llaves AES que utiliza se podía extraer por medio de una vulnerabilidad IDOR. Con la información obtenida de llaves, y con información de logs de su app móvil permiten entender como se implementaba el algoritmo de encripcion. Finalmente se creo un BOT en telegram el cual resolviera los challenges que solicitaba la chapa para poder realizar la apertura. La Metodologia utilizada para el análisis no es nueva, se baso en el trabajo de presentaciones DEFCON anteriores, por lo que referencias a esos trabajo estaran incluidos en la presentación, la intención principal de la platica es que sirva como guía para el futuro análisis de este tipo de dispositivos.

SpeakerBio: Cesar Ortega Ortega, Total Cyber-Sec - Cyber Security Consultant

- Cyber Security Consultant in México
    - ♦ Interested in finding bugs in embedded systems
    - ♦ CTF Player

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 10:50-11:30 PDT

Title: Catch them all! Detection Engineering and Purple Teaming in the Cloud
When: Friday, Aug 9, 10:50 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Where to start looking for attackers in a cloud environment? In a world where cloud providers have hundreds of services and thousands of API calls, getting started can feel overwhelming.

In this talk, we lay out the foundations of a modern detection engineering program built and tailored for the cloud, such as threat-informed defense based on real-world attacker activity, emulating common attacker behavior, shortening feedback loops to validate telemetry, and continuous end-to-end testing of threat detection rules. Additionally, we introduce a new open-source project, Grimoire, which allows leveraging pre-built datasets of AWS CloudTrail logs for common attacks.

You'll gain a hands-on, actionable understanding of how to start identifying threats in your cloud environment, or improve your existing process.

SpeakerBio: Christophe Tafani-Dereeper

Christophe lives in Switzerland and works on cloud security research and open source at Datadog. He previously worked as a software developer, penetration tester and cloud security engineer. Christophe is the maintainer of several open-source projects such as Stratus Red Team, GuardDog, CloudFlair, Adaz, and the Managed Kubernetes Auditing Toolkit (MKAT).

Return to Index - Add to Google - ics Calendar file

PLV - Saturday - 17:00-17:45 PDT

Title: Challenges and Reactions: Cybersecurity and Communications Resilience in Taiwan
When: Saturday, Aug 10, 17:00 - 17:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

</p> **SpeakerBio:** Herming Chiueh, Deputy Minister at Ministry of Digital Affairs, Taiwan

Herming Chiueh received the B.S. degree in electrophysics from National Chiao Tung University, Hsinchu, Taiwan, and the M.S. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, CA, USA. From 1996 to 2002, he was with the Information Sciences Institute, University of Southern California, Marina del Rey, CA, USA. He currently serves as Deputy Minister at Ministry of Digital Affairs, Taiwan. He is currently on-leave from the faculty member of Department of Electrical and Computer Engineering, National Yang Ming Chiao Tung University, Hsinchu, Taiwan.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 10:30-11:15 PDT

Title: Changing Global Threat Landscape with Rob Joyce and Dark Tangent
When: Sunday, Aug 11, 10:30 - 11:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Rob Joyce, former NSA and White House cyber official, will engage with Dark Tangent to analyze the evolving state of global cyber threats. Their discussion will explore the impact and potential of artificial intelligence, assessing how AI is reshaping the cybersecurity landscape and what it means for the future of global security.

Speakers: Rob Joyce,Jeff "The Dark Tangent" Moss

SpeakerBio: Rob Joyce

Rob served over 34 years at the NSA, where he held roles including the head of Tailored Access Operations (TAO), the NSA hackers running operations to produce foreign intelligence. He spent his final years as the head of the Agency's cybersecurity directorate. He also served on the White House National Security Council as a Special Assistant to the President and Cybersecurity Coordinator, as well as Acting Homeland Security Advisor. Throughout his career, he led operations pursuing the most sophisticated hackers and innovated technologies to protect vital national assets — including the the US classified networks and nuclear authorization codes. He remains dedicated to upholding our national security in the cyber realm.

SpeakerBio: Jeff "The Dark Tangent" Moss, DEF CON Communications
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Chasse Partie Systems CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-E - Map

Description:

The inception of this distinctive event occurred at DEF CON 31, initiated by a fortuitous encounter with CookieT while participating in LineCon for merch. Our shared passions fostered an immediate bond, and it was amidst this camaraderie that the idea for a future challenge germinated. Having previously engaged participants with puzzle-embedded challenge coins, I (Chasse) was inspired to expand the concept beyond a mere cipher. The aim was to design a contest that would appeal across a broad spectrum of skill levels by integrating a variety of puzzles, both modern and traditional, to attract a wider audience from a complete beginner new to the hackerspace to the more seasoned and advanced hacker. Observing the collective enthusiasm as participants unraveled the first simple coin puzzle was exhilarating, yet the quick resolution of the puzzle occasionally detracted from the overall experience for more advanced puzzle solvers. Throughout DEF CON 31, CookieT and I explored the feasibility of a web-based challenge CTF, laying the foundation for what would evolve into a pioneering contest and experience. Later Raven emerged from the shadows of cyberspace to help us chisel out the contest from Zeroes and Ones

With the announcement of DEF CON 32's theme, our concept was honed, ready to blend our creative talents into this year's challenge. We crafted an innovative combination of a narrative-driven journey game, scavenger hunt, and web-based Capture The Flag (CTF) challenges, all meticulously aligned with the DEC CON 32 "Engage" theme. This contest emerges as a holistic platform, introducing DEF CON newcomers to core security principles through an engaging narrative. Spanning a variety of fields including OSINT, cryptography, radio, telephony, password, and web security. It promises a rich, diverse experience! Participants, automatically divided into teams, are propelled on a quest to decode puzzles and unearth flags, with challenges designed to suit everyone from novices to veterans seeking sophisticated, intricate challenges. This contest transcends the conventional competition framework, evolving into an artful endeavor that illustrates the symbiosis of storytelling and technical puzzles to create a deeply immersive learning adventure. Imagined as an interactive storybook, it invites attendees to navigate their own routes, making their own choices that lead them through a story-rich exploration of security concepts and engagement even with each other.

The technical infrastructure of this experience is built on varied technologies. The main website, https://www.chassepartie.com, is developed with Ruby on Rails 7.1 and hosted on Heroku, with CloudFlare acting as our Web Application Firewall (WAF). This site functions as the scoreboard and narrative hub of the contest. Additionally, we have set up an XCP-NG hypervisor to host approximately 10 to 15 virtual machines as targets for participant engagement. Augmented reality markers are also in place, intended for deployment in communal areas like sticker boards, to enhance the experience. These elements are interwoven with the storyline, guiding attendees through what we believe is an unprecedented adventure-style CTF challenge named Chasse Partie Systems – Dystopian Apocalypse Resistance Terminal.

So come and join us on our deviant journey, what are you waiting for?

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Chasse Partie Systems CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-E - Map

Description:

The inception of this distinctive event occurred at DEF CON 31, initiated by a fortuitous encounter with CookieT while participating in LineCon for merch. Our shared passions fostered an immediate bond, and it was amidst this camaraderie that the idea for a future challenge germinated. Having previously engaged participants with puzzle-embedded challenge coins, I (Chasse) was inspired to expand the concept beyond a mere cipher. The aim was to design a contest that would appeal across a broad spectrum of skill levels by integrating a variety of puzzles, both modern and traditional, to attract a wider audience from a complete beginner new to the hackerspace to the more seasoned and advanced hacker. Observing the collective enthusiasm as participants unraveled the first simple coin puzzle was exhilarating, yet the quick resolution of the puzzle occasionally detracted from the overall experience for more advanced puzzle solvers. Throughout DEF CON 31, CookieT and I explored the feasibility of a web-based challenge CTF, laying the foundation for what would evolve into a pioneering contest and experience. Later Raven emerged from the shadows of cyberspace to help us chisel out the contest from Zeroes and Ones

With the announcement of DEF CON 32's theme, our concept was honed, ready to blend our creative talents into this year's challenge. We crafted an innovative combination of a narrative-driven journey game, scavenger hunt, and web-based Capture The Flag (CTF) challenges, all meticulously aligned with the DEC CON 32 "Engage" theme. This contest emerges as a holistic platform, introducing DEF CON newcomers to core security principles through an engaging narrative. Spanning a variety of fields including OSINT, cryptography, radio, telephony, password, and web security. It promises a rich, diverse experience! Participants, automatically divided into teams, are propelled on a quest to decode puzzles and unearth flags, with challenges designed to suit everyone from novices to veterans seeking sophisticated, intricate challenges. This contest transcends the conventional competition framework, evolving into an artful endeavor that illustrates the symbiosis of storytelling and technical puzzles to create a deeply immersive learning adventure. Imagined as an interactive storybook, it invites attendees to navigate their own routes, making their own choices that lead them through a story-rich exploration of security concepts and engagement even with each other.

The technical infrastructure of this experience is built on varied technologies. The main website, https://www.chassepartie.com, is developed with Ruby on Rails 7.1 and hosted on Heroku, with CloudFlare acting as our Web Application Firewall (WAF). This site functions as the scoreboard and narrative hub of the contest. Additionally, we have set up an XCP-NG hypervisor to host approximately 10 to 15 virtual machines as targets for participant engagement. Augmented reality markers are also in place, intended for deployment in communal areas like sticker boards, to enhance the experience. These elements are interwoven with the storyline, guiding attendees through what we believe is an unprecedented adventure-style CTF challenge named Chasse Partie Systems – Dystopian Apocalypse Resistance Terminal.

So come and join us on our deviant journey, what are you waiting for?

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Chasse Partie Systems CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-E - Map

Description:

The inception of this distinctive event occurred at DEF CON 31, initiated by a fortuitous encounter with CookieT while participating in LineCon for merch. Our shared passions fostered an immediate bond, and it was amidst this camaraderie that the idea for a future challenge germinated. Having previously engaged participants with puzzle-embedded challenge coins, I (Chasse) was inspired to expand the concept beyond a mere cipher. The aim was to design a contest that would appeal across a broad spectrum of skill levels by integrating a variety of puzzles, both modern and traditional, to attract a wider audience from a complete beginner new to the hackerspace to the more seasoned and advanced hacker. Observing the collective enthusiasm as participants unraveled the first simple coin puzzle was exhilarating, yet the quick resolution of the puzzle occasionally detracted from the overall experience for more advanced puzzle solvers. Throughout DEF CON 31, CookieT and I explored the feasibility of a web-based challenge CTF, laying the foundation for what would evolve into a pioneering contest and experience. Later Raven emerged from the shadows of cyberspace to help us chisel out the contest from Zeroes and Ones

With the announcement of DEF CON 32's theme, our concept was honed, ready to blend our creative talents into this year's challenge. We crafted an innovative combination of a narrative-driven journey game, scavenger hunt, and web-based Capture The Flag (CTF) challenges, all meticulously aligned with the DEC CON 32 "Engage" theme. This contest emerges as a holistic platform, introducing DEF CON newcomers to core security principles through an engaging narrative. Spanning a variety of fields including OSINT, cryptography, radio, telephony, password, and web security. It promises a rich, diverse experience! Participants, automatically divided into teams, are propelled on a quest to decode puzzles and unearth flags, with challenges designed to suit everyone from novices to veterans seeking sophisticated, intricate challenges. This contest transcends the conventional competition framework, evolving into an artful endeavor that illustrates the symbiosis of storytelling and technical puzzles to create a deeply immersive learning adventure. Imagined as an interactive storybook, it invites attendees to navigate their own routes, making their own choices that lead them through a story-rich exploration of security concepts and engagement even with each other.

The technical infrastructure of this experience is built on varied technologies. The main website, https://www.chassepartie.com, is developed with Ruby on Rails 7.1 and hosted on Heroku, with CloudFlare acting as our Web Application Firewall (WAF). This site functions as the scoreboard and narrative hub of the contest. Additionally, we have set up an XCP-NG hypervisor to host approximately 10 to 15 virtual machines as targets for participant engagement. Augmented reality markers are also in place, intended for deployment in communal areas like sticker boards, to enhance the experience. These elements are interwoven with the storyline, guiding attendees through what we believe is an unprecedented adventure-style CTF challenge named Chasse Partie Systems – Dystopian Apocalypse Resistance Terminal.

So come and join us on our deviant journey, what are you waiting for?

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 16:30-16:59 PDT

Title: Chatbots for Cybersecurity
When: Friday, Aug 9, 16:30 - 16:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

In this presentation, we explore the integration of chatbots and large language models (LLMs) like ChatGPT in cybersecurity. We begin by explaining chatbots and LLMs, their operation, and their relevance to cybersecurity. We'll discuss practical applications on both defensive and offensive sides. Defensively, chatbots can automate tasks such as log parsing, web scraping, and data analysis, and aid in educating team members on complex security concepts. Offensively, chatbots can be employed for social engineering, phishing simulations, and automating attack techniques. Real-world examples demonstrate how ChatGPT supports security engineering by generating Python scripts, creating cybersecurity content, and assisting with complex projects. By the end, you'll understand the potential of chatbots and LLMs in enhancing cybersecurity workflows.

SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 16:00-16:59 PDT

Title: Choose your own adventure: Has your fleet been hacked?
When: Saturday, Aug 10, 16:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

This is an audience-participation talk in the style of the 1980s Choose your own Adventure books. We will expose the audience to a quasi real life incident, giving them the choice to choose how they deal with that incident. This will give insight in to the difficult choices that have to be made by operators in real time.

SpeakerBio: Ken Munro, Partner and Founder at Pen Test Partners

Ken Munro is Partner and Founder of Pen Test Partners, a firm of ethical hackers. He and colleagues hold private pilot's licenses and have been interested in aviation security for many years. They also publish and blog about their research into aviation cyber security, covering topics from airborne connectivity, the potential risks of publicly available avionics component information, and even the entire attack surface of the modern airport. Ken and Pen Test Partners have also been invited to speak at various aviation industry events, and on aviation at specialist security events such as DEF CON's Aerospace Village, the Global Connected Aircraft Summit, and the Aviation ISAC Summit among others.

Return to Index - Add to Google - ics Calendar file

HRV - Saturday - 15:00-15:30 PDT

Title: Clapping cheeks, aka home brew antennas
When: Saturday, Aug 10, 15:00 - 15:30 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

Making and deploying double bazooka antenna out of commonly available materials.

SpeakerBio: Seth
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 12:30-13:15 PDT

Title: Clash, Burn, and Exploit: Manipulate Filters to Pwn kernelCTF
When: Sunday, Aug 11, 12:30 - 13:15 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

As the successor to the iptables, nftables stands as a crucial network component within the Linux kernel, managing packet filtering and other network-related functionalities. With continuous development and changes, features designed to increase its efficiency, such as batch commit, anonymous chains/sets, and asynchronous garbage collection, have been implemented, which in turn has significantly increased its complexity and made it an attractive target for attackers in recent years.

Since the announcement of the kernelCTF bug bounty, multiple nftables 0-day vulnerabilities have been reported and patched to enhance its security. However, if not careful enough, the security patch may not only mitigate the bug but also introduce new security issues unintentionally. By researching the structural changes in the nftables codebase, we successfully uncover new vulnerabilities despite the intense competition in kernelCTF. Also, we managed to speedrun the exploitation just before Google removed nftables from LTS instance, becoming the last LTS nftables exploitation.

In this presentation, we will share three nftables vulnerabilities we discovered in a storytelling fashion. We start with a brief introduction on how nftables works under the hood to familiarize attendees with the basics. After that, we dive into nftables internals and dissect three vulnerabilities discovered during our journey, two of which involved utilizing hard-to-exploit race conditions to pwn the flag. Alongside details of the exploitation, we will also share the roller-coaster story of kernelCTF experiences, filled with dramatic highs and lows, making it a tense and exhilarating journey.

- Previous nf_tables research:
- link
- link
- link
- Container escape:
- link
- RCU related documentation:
- link
- link

SpeakerBio: Kuan-Ting "HexRabbit" Chen, Security Researcher at DEVCORE

Kuan-Ting Chen, also recognized as HexRabbit, is a Security Researcher at DEVCORE and a member of the Balsn CTF team. Specializing in low-level exploitation, he is curious about how things work and enjoys the challenge of unraveling the complexities of modern computing systems.

Currently, he focused on the topic of Linux kernel exploitation, his work includes discovering multiple 0-day vulnerabilities in key Linux components like io_uring, ksmbd (an in-kernel SMB server), and the nftables submodule.

Return to Index - Add to Google - ics Calendar file

CLV - Sunday - 12:40-12:59 PDT

Title: Closing Note
When: Sunday, Aug 11, 12:40 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

AIxCC - Friday - 15:00-15:45 PDT

Title: Closing the Software Vulnerability Gap
When: Friday, Aug 9, 15:00 - 15:45 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Our software systems are vulnerable. Imagine a world where they're not. DARPA's Information Innovation Office discusses the agency's mission in closing the software vulnerability gap

SpeakerBio: Dr. Kathleen Fisher, DARPA Information Innovation Office Director at DARPA

Dr. Kathleen Fisher assumed the role of office director for DARPA's Information Innovation Office (I2O) in May 2022. In this position, she leads program managers who are funding the development of programs, technologies, and capabilities to ensure an information advantage for the United States and its allies, and coordinates this work across the Department of Defense and U.S. government.

Fisher was previously the deputy office director for I2O from October 2021 to April 2022. This is Fisher's second tour at DARPA, having previously served as a program manager in I2O from 2011 to 2014. As a program manager, she conceptualized, created, and executed programs in high-assurance computing and machine learning. Her High-Assurance Cyber Military Systems (HACMS) and Probabilistic Programming for Advancing Machine Learning (PPAML) programs continue to benefit the Department of Defense and U.S. commercial industry.

Fisher joined DARPA from Tufts University, where she was a professor in the Department of Computer Science, and served as chair of the department from 2016 to 2021. Earlier in her career, she was a principal member of the technical staff at AT&T Labs.

She is a AAAS fellow, an ACM fellow, and a Hertz Foundation fellow. Fisher has served as chair of the ACM Special Interest Group in Programming Languages (SIGPLAN) and as program chair for three of SIGPLAN's marquee conferences: PLDI, OOPSLA, ICFP. She has also served as an associate editor for TOPLAS and as an editor of the Journal of Functional Programming.

Fisher has long been a leader in the effort to increase diversity and inclusion in computer science. She was co-chair of the Computing Research Association's Committee on the Status of Women (CRA-W) for three years, and she co-founded SIGPLAN's Programming Language Mentoring Workshop (PLMW) series. Fisher is a recipient of the SIGPLAN Distinguished Service Award. She is a past chair of DARPA's Information Science and Technology (ISAT) Study Group and a member of the Board of Trustees of Harvey Mudd College.

Fisher holds a doctorate in computer science from Stanford University.

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 11:15-12:15 PDT

Title: Cloud Native Security Platform for Defenders
When: Friday, Aug 9, 11:15 - 12:15 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

In today's dynamic cybersecurity landscape, organizations and security professionals are constantly seeking innovative approaches to enhance their defensive capabilities. One such approach involves leveraging cloud-native technologies to build a robust platform for security operations and capture the flag (CTF) events. By combining the power of Cilium, Arkime, and Amazon Elastic Kubernetes Service (EKS), you can create a comprehensive solution that empowers security teams with unprecedented visibility, observability, and control over their environments.

Enhancing Security Operations from Layer 3 to Layer 7 This cloud-native platform integrates Cilium, Arkime, and EKS to provide a holistic view of network activities and potential threats from Layer 3 to Layer 7 of the OSI model. Cilium, leveraging eBPF (Extended Berkeley Packet Filter) technology, offers deep visibility into network traffic, enabling security teams to observe and analyze network flows from the Network layer to the Application layer. This allows for the detection of anomalous behavior and the enforcement of security policies at a granular level. Arkime complements this by providing large-scale packet capture and analysis, allowing security professionals to perform in-depth forensic analysis and threat hunting. By integrating Arkime with Cilium, security teams can seamlessly correlate network flows with packet data, offering a comprehensive understanding of network activities.

Scalability, Flexibility, and Community Collaboration Amazon EKS underpins this platform, providing a scalable and resilient infrastructure for deploying and managing Kubernetes clusters. This enables security teams to focus on core operations without worrying about the underlying infrastructure. The platform's scalability ensures it can handle large-scale CTF events or security incidents. During the Defcon Blue Team Village talk, attendees will learn about the integration and deployment process of this platform, including the challenges faced and solutions implemented. Post-conference, the platform will be released for public use, allowing the security community to leverage, contribute to, and enhance this innovative solution for their own security operations and CTF events. This collaborative effort aims to collectively advance the capabilities of cloud-native security platforms.

In today's dynamic cybersecurity landscape, organizations and security professionals are constantly seeking innovative approaches to enhance their defensive capabilities. One such approach involves leveraging cloud-native technologies to build a robust platform for security operations and capture the flag (CTF) events. By combining the power of Cilium, Arkime, and Amazon Elastic Kubernetes Service (EKS), you can create a comprehensive solution that empowers security teams with unprecedented visibility, observability, and control over their environments.

SpeakerBio: Dafinga
No BIO available

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 12:30-12:59 PDT

Title: Cloud Offensive Breach and Risk Assessment (COBRA)
When: Friday, Aug 9, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Cloud Offensive Breach and Risk Assessment (COBRA) is an open-source tool designed to empower users to simulate attacks within multi-cloud environments, offering a comprehensive evaluation of security controls. By automating the testing of various threat vectors including external and insider threats, lateral movement, and data exfiltration, COBRA enables organizations to gain insights into their security posture vulnerabilities. COBRA is designed to conduct simulated attacks to assess an organization's ability to detect and respond to security threats effectively.

It facilitates Proof of Concept (POC) evaluations, assesses security controls, measures maturity levels, and generates comprehensive reports, enabling organizations to enhance their cloud security resilience through lifelike threat scenarios.

COBRA Features:

Seamless Integration for POC and Tool Evaluation: COBRA provides seamless integration for Proof of Concept (POC) and tool evaluation purposes. Whether you're exploring new cloud-native applications or evaluating existing solutions, COBRA offers a user-friendly interface and flexible deployment options to facilitate effortless testing and assessment. Comprehensive Assessment of Cloud-Native Security Posture: Gain unparalleled insights into your organization's existing cloud-native security posture with COBRA. Our advanced assessment capabilities enable you to identify vulnerabilities, assess security controls, and pinpoint areas for improvement. By understanding your current security posture, you can proactively address gaps and strengthen your defenses against emerging threats. Benchmarking Against Industry Standards and Best Practices: COBRA enables you to benchmark your cloud security controls against industry standards and best practices. With our comprehensive benchmarking framework, you can compare your security posture against established benchmarks, identify areas of strength and weakness, and prioritize remediation efforts accordingly. Actionable Insights and Recommendations: COBRA goes beyond providing insights by providing a report delivering actionable recommendations tailored to your organization's specific needs. Whether it's optimizing security configurations, implementing additional controls, or enhancing incident response processes, COBRA equips you with the tools and guidance needed to bolster your cloud security defenses.

Continuous Threat Simulation: COBRA offers a modular and templatized approach for users to easily integrate additional modules, allowing for continuous threat simulation and adaptability, by providing a flexible framework for adding modules, COBRA ensures that users can tailor their threat simulation capabilities according to evolving security needs, making it an ideal platform for continuous threat simulation.

Speakers:
Harsha Koushik,Anand Tiwari

SpeakerBio:
Harsha Koushik

Harsha Koushik is a security engineer and researcher, passionate about securing digital systems. Specializing in Cloud-Native Application Platform Protection (CNAPP), tackling emerging cyber threats while working at large scales. Additionally, Harsha hosts the security podcast 'Kernel-Space,' exploring insightful discussions on the latest trends and issues in cybersecurity.

SpeakerBio:
Anand Tiwari

Anand Tiwari is an information security professional with a strong technical background working as a Product Manager (PM), focusing on the more technical aspects of a cloud security product. He tries to fill it in by doing in-depth technical research and competitive analysis, given business issues, strategy, and a deep understanding of what the product should do and how the

products actually work. He has authored ArcherySec—an open source-tool and has presented at BlackHat, DEF CON USA, and HITB conferences. He has successfully given workshops at many conferences such as DevOpsDays Istanbul, Boston.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 10:00-11:45 PDT

Title: Cloud Offensive Breach and Risk Assessment (COBRA)
When: Friday, Aug 9, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W308 - Map

Description:

Cloud Offensive Breach and Risk Assessment (COBRA) is an open-source tool designed to empower users to simulate attacks within multi-cloud environments, offering a comprehensive evaluation of security controls. By automating the testing of various threat vectors including external and insider threats, lateral movement, and data exfiltration, CNBAS enables organizations to gain insights into their security posture vulnerabilities. CNBAS is designed to conduct simulated attacks to assess an organization's ability to detect and respond to security threats effectively.

Speakers: Anand Tiwari,Harsha Koushik

SpeakerBio: Anand Tiwari

Anand Tiwari is an information security professional with a strong technical background working as a Product Manager (PM), focusing on the more technical aspects of a cloud security product. He tries to fill it in by doing in-depth technical research and competitive analysis, given business issues, strategy, and a deep understanding of what the product should do and how the products actually work. He has authored ArcherySec—an open source-tool and has presented at BlackHat, DEF CON USA, and HITB conferences. He has successfully given workshops at many conferences such as DevOpsDays Istanbul, Boston.

SpeakerBio: Harsha Koushik

Harsha Koushik is a security engineer and researcher, passionate about securing digital systems. Specializing in Cloud-Native Application Platform Protection (CNAPP), tackling emerging cyber threats while working at large scales. Additionally, Harsha hosts the security podcast 'Kernel-Space,' exploring insightful discussions on the latest trends and issues in cybersecurity.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 14:00-14:50 PDT

Title: Cloud Offensive Breaches: The Graph-Based Exploitation of Misconfigurations
When: Saturday, Aug 10, 14:00 - 14:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

During this talk, we will cover the critical importance of permissions management in integrations, especially in cloud environments, and how an inappropriate permissions standard can create significant vulnerabilities for attackers. We will explore how an attacker can leverage legitimate permissions to perform privilege escalation in the cloud, highlighting the fundamental differences between Attack Vector and Attack Path. Additionally, we will examine the most effective and shortest path an attacker can take to achieve success in their goals. We will also discuss strategies to improve security in this context and mitigate these threats.

SpeakerBio: Filipi Pires, Founder at Black&White Technology

I’ve been working as Security and Threat Researcher and Cybersecurity Advocate at senhasegura, Founder at Black&White Technology, Cybersecurity Advocate, Snyk Ambassador, Application Security Specialist and Hacking is NOT a crime Advocate. International Speaker at Security and New technologies events in many countries such as US, Canada, France, Spain, Germany, Poland, and others, I’ve served as University Professor in Graduation and MBA courses at Brazilian colleges, in addition, I'm Creator and Instructor of the Course - Malware Attack Types with Kill Chain Methodology (PentestMagazine), PowerShell and Windows for Red Teamers(PentestMagazine) and Malware Analysis - Fundamentals (HackerSec).

Return to Index - Add to Google - ics Calendar file

CLV - Sunday - 10:00-10:35 PDT

Title: Cloud Tripwires: fighting stealth with stealth
When: Sunday, Aug 11, 10:00 - 10:35 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Cloud attacks continue to evolve e.g., AWS enumeration without logging (Fourchette), Azure OAuth tokens used for EoP and persistence (Blizzard), Cloud Shell backdoors, code abuse in GSuite scripting (Bryant), and tool evolution (Rhinolabs pacu), with current defensive approaches of lagging further and further behind.

This talk covers research and tooling to improve cloud defenses in AWS, Azure, and GCP, using more stealthy measures which complement existing techniques. We call the approach cloud tripwires, which involves stealthy defensive techniques that can provide low-FP detections of malicious actors.

Through analysis of cloud provider IAM design, published attack techniques and common attack tools, we show multiple stealthy detection techniques such as: restricted admin roles that are not used by valid users; seeding of the restricted admin roles in regular user policies; honey resources (buckets, files) with detections to flag access; seeding of honey resources within user policies; cached honey credentials seeded in CLI installations in external client environments, EC2 instances, and Cloud Shells; unrestricted cross-account roles to restricted accounts; metadata proxy/iptables config on EC2 instances that issue restricted temporary tokens; and full CRUD/reporting/auditing functionality.

SpeakerBio: Jenko Hwong

Jenko Hwong is a Principal Researcher on Netskope's Threat Research Team, focusing on cloud threats/vectors and identity abuse. He's spent time in engineering and product roles at various security startups in vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-23:59 PDT

Title: Cloud Village CTF
When: Friday, Aug 9, 10:00 - 23:59 PDT
Where: Virtual

Description:

If you ever wanted to break stuff on the cloud, or if you like rabbit holes that take you places you did not think you would go to, follow complicated story lines to only find you could have reached to the flag without scratching your head so much - then this CTF is for you!

Our CTF is a two days jeopardy style contest where we have a bunch of challenges hosted across multiple Cloud providers across multiple categories of difficulty.

You can register as teams or go solo, use hints or stay away from them, in the end it will be all for glory or nothing. Plus the prizes. Did we not mention the prizes? :D

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Cloud Village CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

If you ever wanted to break stuff on the cloud, or if you like rabbit holes that take you places you did not think you would go to, follow complicated story lines to only find you could have reached to the flag without scratching your head so much - then this CTF is for you!

Our CTF is a two days jeopardy style contest where we have a bunch of challenges hosted across multiple Cloud providers across multiple categories of difficulty.

You can register as teams or go solo, use hints or stay away from them, in the end it will be all for glory or nothing. Plus the prizes. Did we not mention the prizes? :D

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Cloud Village CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

If you ever wanted to break stuff on the cloud, or if you like rabbit holes that take you places you did not think you would go to, follow complicated story lines to only find you could have reached to the flag without scratching your head so much - then this CTF is for you!

Our CTF is a two days jeopardy style contest where we have a bunch of challenges hosted across multiple Cloud providers across multiple categories of difficulty.

You can register as teams or go solo, use hints or stay away from them, in the end it will be all for glory or nothing. Plus the prizes. Did we not mention the prizes? :D

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: CMD+CTRL at DEF CON 32
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-D - Map

Description:

CMD+CTRL Web App Hacking Challenge gives you the opportunity to showcase your red team skills by attacking real web applications. The CMD+CTRL platform is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real world systems at risk.

At DEF CON 32: We will be replaying some of our Cyber Range Greatest Hits. We will be running 4 different Ranges with over a 150 challenges possible!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: CMD+CTRL at DEF CON 32
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-D - Map

Description:

CMD+CTRL Web App Hacking Challenge gives you the opportunity to showcase your red team skills by attacking real web applications. The CMD+CTRL platform is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real world systems at risk.

At DEF CON 32: We will be replaying some of our Cyber Range Greatest Hits. We will be running 4 different Ranges with over a 150 challenges possible!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: CMD+CTRL at DEF CON 32
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-D - Map

Description:

CMD+CTRL Web App Hacking Challenge gives you the opportunity to showcase your red team skills by attacking real web applications. The CMD+CTRL platform is a hacking game designed to teach the fundamentals of web application security. Explore vulnerable web applications, discover security flaws, and exploit those flaws to earn points and climb up the scoreboard. After attacking an application for yourself, you'll have a better understanding of the vulnerabilities that put real world systems at risk.

At DEF CON 32: We will be replaying some of our Cyber Range Greatest Hits. We will be running 4 different Ranges with over a 150 challenges possible!

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 12:00-13:45 PDT

Title: CODASM - Hiding Payloads in Plain .text
When: Saturday, Aug 10, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W305 - Map

Description:

CODASM aims to decrease a stageless payload's Shannon entropy, which was found to be a simple but annoying detection vector used by EDRs. It's a Python program that processes arbitrary binary inputs and produces a C program consisting of two parts: a buffer holding generated x86-64 ASM instructions with the original payload encoded into it, and a set of functions that can decode the ASM at runtime. The buffer is designed to be compiled into the final payload's .text section, thus it looks like regular (if not functional) code to AVs, EDRs and analysts. This encoding effectively decreases the payload's Shannon entropy but comes with a significant increase in output size. The demo will cover usage of the tool and dissection/reverse engineering of the resulting payload.

SpeakerBio: Moritz Laurin Thomas, Senior Red Team Security Consultant at NVISO ARES

Moritz is a senior red team security consultant at NVISO ARES (Adversarial Risk Emulation & Simulation). He focuses on research & development in red teaming to support, enhance and extend the team's capabilities in red team engagements of all sorts. Before joining the offensive security community, Moritz worked on a voluntary basis as a technical malware analyst for a well-known internet forum with focus on evading detections and building custom exploits. When he isn't infiltrating networks or exfiltrating data, he is usually knees deep in research and development, dissecting binaries and developing new tools.

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 15:30-16:30 PDT

Title: Cognative Weather Report
When: Saturday, Aug 10, 15:30 - 16:30 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

We are living through a time period where not only are wars being fought, on land, sea, air, and cyber, but we have all been drafted into a misinformation, disinformation, and malinformation war that many of us were not given the proper tools or training for. The times we exist in are unprecedented, and the more that people primarily consume their information online, the more susceptible we all are to becoming influenced by operations that are coming foreign adversaries as a means of not only spreading misinformation, disinformation, and malformation, but as means of dividing and polarizing our nation. How can we resist that? What can we look for? Is there a framework the average voter can use? Join us for this fireside chat to learn more and equip yourself for the upcoming election.

Speakers: Constantine Nicolaidis,Catherine Terranova

SpeakerBio: Constantine Nicolaidis

Constantine leads a Risk Management practice that focuses on securing U.S. privately owned critical infrastructure. Over the last decade he has leveraged his expertise in security and data-based product development to create tools for security professionals. Constantine has also spent the last 5 years developing a geopolitical modeling system to help forecast and describe the nature of political and social crises. He advises various security groups on the nature of modern multi-domain warfare with an emphasis on the cyber and cognitive domains. Constantine holds a Master's Degree in Human-Computer Interaction from the Carnegie Mellon School of Computer Science and is currently enrolled in the Master's in Cybersecurity Degree program at the SANS Technology Institute.

SpeakerBio: Catherine Terranova

Catherine Terranova is a Columbia University alumna and researcher. Her current focus is on cyber security and election integrity with an emphasis on misinformation, disinformation, and malinformation, known as information integrity. Ms. Terranova joined the team in 2021 and has been growing and developing the Voting Village since DEF CON 29. She heads all aspects of the program and manages other related projects focused on the global preservation of democracy.

Return to Index - Add to Google - ics Calendar file

SEV - Saturday - 15:30-17:30 PDT

Title: Cold Calls
When: Saturday, Aug 10, 15:30 - 17:30 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Come make a call in front of our soundproof booth. We provide everything, the target company, their phone number, and three objectives to gather (easy, medium, and hard). First come, first serve.

Return to Index - Add to Google - ics Calendar file

SEV - Saturday - 13:00-14:59 PDT

Title: Cold Calls
When: Saturday, Aug 10, 13:00 - 14:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Come make a call in front of our soundproof booth. We provide everything, the target company, their phone number, and three objectives to gather (easy, medium, and hard). First come, first serve.

Return to Index - Add to Google - ics Calendar file

SEV - Sunday - 11:30-13:59 PDT

Title: Cold Calls
When: Sunday, Aug 11, 11:30 - 13:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Come make a call in front of our soundproof booth. We provide everything, the target company, their phone number, and three objectives to gather (easy, medium, and hard). First come, first serve.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 14:00-14:59 PDT

Title: Color Blasted Badge Making: How Hard Could It Be ?
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Without plan or intent, three Makers took three paths to achieve colorful badges and none were smart enough to turn back. Join our panel discussion to learn our different approaches, the strengths and weaknesses of each, and ask your probing questions. Perhaps you too will be foolish enough to venture into the technicolor labyrinth.

Speakers:
Abhinav Panda,Bradán Lane,Hamster

SpeakerBio: Abhinav Panda

Abhinav's artistry comes from the times he used to sneakily paint drawings made by his sister. His hacking career began as a toddler, disassembling his toys but never put them back together. His entrepreneurial roots come from selling snacks at a school fair and making a loss of $10. Having learned how not to make money, he launched Hackerware.io and the rest, as they say, is history.

SpeakerBio: Bradán Lane

Bradán graduated third grade with a degree in crayon. This, combined with his unwavering belief in "how difficult could it be", makes him eminently qualified to speak on the nuances of color theory in electronics design.

SpeakerBio: Hamster

Hamster is an engineer who watched too much MacGyver as a kid and is now doomed to invent more and more complicated ways to make the Angry Pixies dance.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 14:00-14:50 PDT

Title: Combining Uncensored and Censored LLMs for Ransomware Generation
When: Saturday, Aug 10, 14:00 - 14:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

Uncensored LLMs represent a category of language models free from ethical constraints, thus prone to misuse for various malicious purposes like generating malware. However, their capabilities fall short compared to commercially available LLMs, which are censored and unsuitable for such nefarious activities. Previously, researchers could bypass censorship in LLMs to generate malicious content using Jail Breaks. However, over time and with the introduction of new security measures, such exploits have become increasingly rare. In this research, we propose a novel technique in which we combine censored and uncensored LLMs for the generation of ransomware. The uncensored LLM will generate the initial malware, which will then be refined by the censored LLM to create a final, functional ransomware. We have tested the developed Ransomware in latest version of Windows OS and found it suitable for exploitation purposes. Additionally with minor efforts the rasnowmares can be updated using LLM for code obfuscation and unnecessary functionality addition for bypassing antivirus and antimalware solutions.

SpeakerBio: Muhammad Mudassar Yamin
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Compromising an Electronic Logging Device and Creating a Truck2Truck Worm
When: Saturday, Aug 10, 16:00 - 16:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

Presented by Jake Jepson and Rik Chatterjee, two Systems Engineering Master's students at Colorado State University, this talk delves into the critical security implications within the trucking industry, particularly focusing on Electronic Logging Devices (ELDs). These devices, integral to compliance with Hours of Service regulations, present unique cyber-physical threats due to their networked nature and lack of standardized security protocols.

The presentation will walk through examining potential remote exploits via wireless ELD compromise, leading to cyber physical control payloads and even wormable scenarios. Key vulnerabilities identified include insecure defaults and poor security practices shown on a commercially available ELD. These vulnerabilities not only expose truck networks to potential unauthorized control but also highlight systemic issues in device certification and security oversight.

The talk will cover their journey from acquiring and reverse engineering ELDs, discovering their common architectures and weaknesses, to demonstrating proof of concept attacks that underline the urgent need for industry-wide security reforms. Notably, Jepson will discuss his first CVE, detailing the coordinated disclosure process and subsequent manufacturer response.

This session is semi-technical, ideal for cybersecurity professionals and amateurs alike, interested in vehicle network protocols, and embedded systems security. Prior knowledge of network protocols such as CAN and J1939, along with an understanding of firmware reverse engineering, will enhance the learning experience, but is not required. Tools and techniques used include network scanners, reverse engineering platforms like Ghidra, and various wireless communication methods.

By attending this presentation, participants will not only understand the specific security flaws affecting heavy vehicles but also appreciate the broader implications for embedded systems security in transportation. This talk is a call to action for improving security practices and regulatory standards in an increasingly interconnected world.

1. Bureau of Transportation Statistics, United States Department of Transportation. "National Transportation Statistics (NTS)." Accessed December 19, 2023. link. doi:10.21949/1503663
2. “Economics and Industry Data.” American Trucking Associations. [Online]. Available: link
3. Technology, Syrma Sgs. “Automotive ECU: The Core Component for Connected Cars.” Electronic Manufacturing Services - Syrma SGS Technology, 15 July 2021, link. Picture: “M156 ECU Upgrade.” DYNE Performance, link. Accessed 22 Apr. 2022.
4. “J1939-13.” SAE International.
5. “Moving Ahead for Progress in the 21st Century Act (MAP-21).” U.S. Department of Transportation. [Online]. Available: Moving Ahead for Progress in the 21st Century Act (MAP-21)
6. “ELD List.” FMCSA. [Online]. Available: link
7. link
8. link
9. link
10. link

Speakers: Jake Jepson,Rik Chatterjee

SpeakerBio: Jake Jepson, Graduate Research Assistant, Department of Systems Engineering at Colorado State University

Currently, Jake serves as a graduate research assistant in the Department of Systems Engineering, working under the guidance of Dr. Jeremy Daily. His role involves collaborating with a team of skilled professionals to conduct research on cybersecurity

and digital forensics within the heavy vehicle industry. Jake's academic journey has emphasized the significance of pursuing a career he is passionate about, and this position has further solidified his love for collaborative problem-solving.

SpeakerBio: Rik Chatterjee, Graduate Research Assistant, Department of Systems Engineering at Colorado State University

Currently, Rik serves as a graduate research assistant in the Department of Systems Engineering at Colorado State University, working under Dr. Jeremy Daily. His role involves research on security of protocol implementations and cybersecurity in the domain of commercial heavy and medium duty vehicles. Driven by a passion for securing embedded systems, Rik's work emphasizes the importance of robust security measures in protecting critical transportation infrastructure against emerging cyber threats.

Return to Index - Add to Google - ics Calendar file

AIV - Saturday - 13:30-14:30 PDT

Title: ConfusedPilot: Data Corruption and Leakage by Misusing Copilot for Microsoft 365
When: Saturday, Aug 10, 13:30 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

The hype for integrating artificial intelligence into an enterprise's daily work has become more prevalent after introducing AI-driven systems that use Retrieval Augmented Generation (RAG), such as Copilot for Microsoft 365. But is the trust in such systems and their control over decision-making processes within enterprises rational? Copilot and other RAG-based systems can be misused to cause dissemination of misinformation that negatively impacts decision-making processes without proper auditing and safeguarding of data available to large language models in RAG-based systems.

This talk will demonstrate such an attack that we have termed ConfusedPilot because of its ability to turn Copilot into a confused deputy. The attack occurs when a malicious document is introduced to the data pool (documents, presentations, other relevant files, etc.) related to a topic affecting the enterprise's decision-making process. The malicious document contains a combination of corrupt data and malicious strings that suppress the correct documents related to the topic and respond to the user's query with only the information present within the malicious document. Furthermore, the talk highlights how this attack can persist after deleting content within the malicious document or the document itself. The talk also points to the larger implications of such attacks, highlighting their cascading effect and existing security measures that can be used to reduce the attack's effectiveness. Our talk sheds light on the current attacks and potential security measures that can shield enterprises from the adverse effects of such attacks on their AI-driven systems.

Speakers: Ayush RoyChowdhury,Mulong Luo,Mohit Tiwari

SpeakerBio: Ayush RoyChowdhury, The University of Texas at Austin
No BIO available
SpeakerBio: Mulong Luo, The University of Texas at Austin
No BIO available
SpeakerBio: Mohit Tiwari, The University of Texas at Austin
No BIO available

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 13:50-15:50 PDT

Title: Connecting the Dots: Mastering Alert Correlation for Proactive Defense in the Cloud
When: Saturday, Aug 10, 13:50 - 15:50 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Interpret the vast amount of alerts (from different sources) received with a comprehensive, hands-on autonomous attack correlation & false positive detection workshop designed to enhance your proactive defense in the cloud. The workshop aims to demystify the process of identifying coordinated attacks amidst this noise, empowering attendees to improve their efficacy & utilize the cloud cost-effectiveness.

No data science expertise is required. Little cloud & secops expertise is required.

Intro: - The session begins with a foundational overview of event analysis challenges and state of the art. - Participants will learn about the ATT&CK framework, focusing on its Flows, Tactics, & Techniques to standardize threat detection.

AI & Data: - A deep dive into accessible open-source AI tools will follow, featuring clustering algorithms, natural language processing, & Markov chains. - Guidance on importing, cleaning, & normalizing data will ensure accuracy in subsequent analyses. - Participants will have access to a demo environment to apply these tools interactively.

Mapping Alerts: - Techniques for automated mapping of alerts to ATT&CK will be demonstrated. - Attendees will engage in mapping exercises using AI.

Clustering Alerts: - The workshop will cover clustering methods based on temporal, spatial, & technical attributes. - Participants will engage in clustering sample alerts to form contextualized attack steps.

Correlating Alerts: - The importance of killchains in cybersecurity will be highlighted, with methods to link attack steps into cohesive killchains. - Participants are guided in creating & analyzing killchains to identify coordinated attacks.

Tickets: - Criteria for creating FP Tickets, Incident Tickets, & Attack Story Tickets will be outlined. - Participants will engage in generating sample tickets, ensuring each type is comprehensive & actionable.

Integrating & QA: - The session will cover integration into existing SOC setups & automation using scripts & tools. - Demonstrations will show how to maintain & update the system for continuous improvement, emphasizing cost-effective cloud automation. - QA, troubleshooting, & further resources.

By the end of this interactive workshop, participants will have experience with AI tools mapping alerts to Techniques, clustering them into contextualized attack steps, & constructing comprehensive killchains to uncover coordinated attacks. Additionally, they will learn to generate actionable tickets for immediate response & long-term improvements in their security posture, all without needing advanced data science knowledge. This session encourages practical application in participants' environments & further exploration of the vast capabilities of open-source AI in cybersecurity, & showcases the power of cloud cost-effectiveness in big data analytics (sagemaker, s3, lambda, etc.).

SpeakerBio: Ezz Tahoun

Ezz Tahoun, a distinguished cyber-security data scientist, who won AI & innovation awards at Yale, Princeton and Northwestern. He also got innovation awards from Canada’s Communications Security Establishment, Microsoft US, Trustwave US, PIA US, NATO, and more. He ran data science innovation programs and projects for OrangeCyber Defense, Forescout Technologies, Royal bank of Canada, Governments, and Huawei Technologies US. He has published 20 papers, countless articles and 15 open source projects in the domain. When he was 19 years old he started his CS PhD in one of the top 5 labs in the world for cyber & AI, in the prestigious University of Waterloo, where he published numerous papers and

became a reviewer for top conferences. His designations include: SANS/GIAC-Advisory-Board, aCCISO, CISM, CRISC, GCIH, GFACT, GSEC, CEH, GCP-Professional-Cloud-Architect, PMP, BENG and MMATH. He was an adjunct professor of cyber defense and warfare at Toronto's school of management.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 13:30-14:45 PDT

Title: Contest Closing Ceremonies and Awards
When: Sunday, Aug 11, 13:30 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 1/Tracks 1-2 - Map

Description:

Return to Index - Add to Google - ics Calendar file

AIxCC - Saturday - 15:00-15:30 PDT

Title: Contextualizing Open Source Software's Importance to CISA's Mission
When: Saturday, Aug 10, 15:00 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:
SpeakerBio: Aeva Black, DHS Cyber Security and Infrastructure Security Agency

Aeva Black is an open-source hacker and international public speaker with 25 years of experience building digital infrastructure and leading open-source projects. They previously served on the OpenSSF Technical Advisory Committee, OpenStack Technical Committee, Kubernetes Code of Conduct Committee, and led open-source security strategy within the Microsoft Azure Office of the CTO. In their spare time, Aeva serves on the Board of the Open-Source Initiative and enjoys riding motorcycles and supporting the local LGBTQ+ community.

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 14:00-15:59 PDT

Title: CopyCat: An Artist Guide to Adversary Forgery
When: Saturday, Aug 10, 14:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

Skills are learned, but application is art. Much like an artist learning the skill to draw, in this workshop, we learn the skill to identify and create byte-sized adversary emulation-based tests. By reading a report with the lens of MITRE ATT&CK, we identify procedures that link back to MITRE ATT&CK techniques or sub-techniques, which allows us to create an atomic red team test based on the reporting. However, like every artist faces when putting pen to paper, the skill of drawing is not the same as the skill of creating. Using art forgery concepts to help us overcome these obstacles, we walk through how to navigate the gaps in reporting and emulate versus simulating the adversary. Participants are encouraged to finish out the atomic tests and contribute to the public Atomic Red Team GitHub. Welcome to the club of legal copycats. Intended audience: International audience with English is a second language. Beginner to intermediate skill. Basic level of programing knowledge and cyber security concepts required. Students are expected to provide their own laptop. Have a GitHub account & understand the clone, git and pull commands.

SpeakerBio: Cat Self, Principal Adversary Emulation Engineer (MITRE ATT&CK)

Cat Self is a Principal Adversary Emulation Engineer working as the macOS/Linux Lead for ATT&CK®, malware developer for MITRE ATT&CK® Evaluations, and SME for International Programs. Cat started her cyber security career at Target and has worked as a developer, internal red team operator, and threat hunter. Cat is a former military intelligence veteran and pays it forward through mentorship, workshops, and public speaking. Outside of work, she is often planning an epic adventure, climbing mountains in foreign lands, learning Chinese, or meeting great people salsa dancing.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 16:00-16:55 PDT

Title: Correlating & contextualizing OT events/alerts/logs using weakly supervised AI
When: Friday, Aug 9, 16:00 - 16:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

In the complex landscape of modern cybersecurity, identifying coordinated attacks within massive volumes of operational & security data is a formidable challenge. Security professionals often grapple with distinguishing these attacks from numerous false positives and isolated incidents. This talk will illuminate how data science can be harnessed to transform tons of ICS events, logs, and alerts into a bunch of clusters, a few kill chains, and fewer actionable insights, with open-source models.

Join us on a journey to enhance ICS security operations efficacy and efficiency.

In the intricate and ever-evolving landscape of modern cybersecurity, pinpointing coordinated attacks amid vast volumes of security data is an immensely challenging task. Security professionals constantly wrestle with distinguishing genuine threats from a sea of false positives and isolated incidents. This talk will shed light on how data science can be leveraged to transform an overwhelming number of events, logs, and alerts into manageable clusters, insightful kill chains, and actionable insights using open-source models.

Attendees will gain a comprehensive understanding of the necessary steps to preprocess and normalize diverse data sources, map them to standardized threat models, and use AI-driven methods to contextualize and correlate security events. The session will also cover how to generate different types of tickets, such as false positive advisories, incident reports, and detailed attack stories, to streamline response efforts and enhance IT & OT security operations' overall efficacy and efficiency.

SpeakerBio: Ezz Tahoun

Ezz Tahoun, a distinguished cyber-security data scientist, who won AI & innovation awards at Yale, Princeton and Northwestern. He also got innovation awards from Canada’s Communications Security Establishment, Microsoft US, Trustwave US, PIA US, NATO, and more. He ran data science innovation programs and projects for OrangeCyber Defense, Forescout Technologies, Royal bank of Canada, Governments, and Huawei Technologies US. He has published 20 papers, countless articles and 15 open source projects in the domain. When he was 19 years old he started his CS PhD in one of the top 5 labs in the world for cyber & AI, in the prestigious University of Waterloo, where he published numerous papers and became a reviewer for top conferences. His designations include: SANS/GIAC-Advisory-Board, aCCISO, CISM, CRISC, GCIH, GFACT, GSEC, CEH, GCP-Professional-Cloud-Architect, PMP, BENG and MMATH. He was an adjunct professor of cyber defense and warfare at Toronto’s school of management.

Return to Index - Add to Google - ics Calendar file

ADV - Sunday - 10:00-11:59 PDT

Title: Correlating slow & stealthy APT traces hiding in the sheer noise
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:
SpeakerBio: Ezz Tahoun

Ezz Tahoun, a distinguished cyber-security data scientist, who won AI & innovation awards at Yale, Princeton and Northwestern. He also got innovation awards from Canada's Communications Security Establishment, Microsoft US, Trustwave US, PIA US, NATO, and more. He ran data science innovation programs and projects for OrangeCyber Defense, Forescout Technologies, Royal bank of Canada, Governments, and Huawei Technologies US. He has published 20 papers, countless articles and 15 open source projects in the domain. When he was 19 years old he started his CS PhD in one of the top 5 labs in the world for cyber & AI, in the prestigious University of Waterloo, where he published numerous papers and became a reviewer for top conferences. His designations include: SANS/GIAC-Advisory-Board, aCCISO, CISM, CRISC, GCIH, GFACT, GSEC, CEH, GCP-Professional-Cloud-Architect, PMP, BENG and MMATH. He was an adjunct professor of cyber defense and warfare at Toronto's school of management.

Return to Index - Add to Google - ics Calendar file

ICSV - Sunday - 10:00-10:55 PDT

Title: Countdown to Industrial Extinction
When: Sunday, Aug 11, 10:00 - 10:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

ICS/OT environments are targets. Since the Colonial Pipeline breach in 2021, the ICS/OT threat landscape has changed tremendously. This presentation is not about the Fear, Uncertain and Doubt when an ICS/OT environment goes boom, but what happens when it goes down for ten days. What's the impact to the organization? It's employees? The people it serves?

Most importantly, what can we do to prevent it from occurring?

The remainder of the presentation covers secure network architecture, therapy for IT and OT working together and continually learning/improving.

SpeakerBio: Mike Holcomb, Fellow of Cybersecurity and ICS/OT Cybersecurity Global Lead at Fluor

Mike helps people learn how to secure Industrial Control Systems (ICS)/Operational Technology (OT) environments, from engineers and IT cyber security team members to asset owners and operators. He is the Fellow of Cybersecurity and the ICS/OT Cybersecurity Global Lead for Fluor, one of the world's largest engineering, procurement, and construction companies. His current role provides him with the opportunity to work in securing some of the world's largest ICS/OT environments, from power plants and commuter rail to manufacturing facilities and refineries. He has his Masters degree in ICS/OT cybersecurity from the SANS Technology Institute. Additionally, he maintains more than a few cyber security and ICS/OT certifications.

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 15:30-16:30 PDT

Title: Covert Quantum Communication
When: Saturday, Aug 10, 15:30 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Given access to the start time, duration, method of encoding, and an all-powerful quantum receiver, could you perform the "simple" task of detecting whether two or more parties were attempting to communicate? Covert communication, or low probability of detection, demonstrates that it is possible to hide signals within noise so effectively that even an all-powerful quantum adversary would have a vanishing probability of detecting the signal's presence. In this talk, I'll provide a high-level overview of covert communication and its extension to the quantum regime. I'll discuss the theoretical underpinnings of covert quantum communication, and how we can practically implement such a system. Finally, I'll discuss the ethical considerations of this work and why we should care about it.

SpeakerBio: Evan Anderson

Driven by a deep curiosity about the nature of information, Evan Anderson transitioned from software engineering to pursue a PhD in quantum information theory and photonic quantum information processing. He is curious about all aspects of information, from its fundamental structure within physics to how we manipulate it to suit our needs in day-to-day conversations. Evan is currently in his final year as a PhD student at the University of Arizona, the home of the Center for Quantum Networks, where his research primarily focuses on covert communication over quantum channels and quantum coding theory.

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 10:00-10:02 PDT

Title: CPV: Day 1 Welcome
When: Friday, Aug 9, 10:00 - 10:02 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Welcome to the 11th CPV at DEF CON! This will be the absolute fastest state of the village sharing talks for the day, plus what's available at the village.

Return to Index - Add to Google - ics Calendar file

CPV - Saturday - 10:25-10:30 PDT

Title: CPV: Day 2 Welcome
When: Saturday, Aug 10, 10:25 - 10:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Welcome to Day 2 of the 11th CPV at DEF CON! A brief overview of the state of the village, talks for the day, plus what's available at the village and what's gone, we might actually run out of friendship bracelet supplies this time around…

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 13:00-13:15 PDT

Title: CPV: Intro to Cyphers
When: Friday, Aug 9, 13:00 - 13:15 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Are you getting stuck on solving ciphers in challenges? Not sure who or what Caesar is? What is "polyalphabetic" or "transposition"? Is this even relevant to modern day cryptography? Come on over for the Intro to Ciphers talk! Talk time: 5-15 minutes

Return to Index - Add to Google - ics Calendar file

CPV - Saturday - 10:30-10:45 PDT

Title: CPV: Intro to Cyphers
When: Saturday, Aug 10, 10:30 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Are you getting stuck on solving ciphers in challenges? Not sure who or what Caesar is? What is "polyalphabetic" or "transposition"? Is this even relevant to modern day cryptography? Come on over for the Intro to Ciphers talk! Talk time: 5-15 minutes

Return to Index - Add to Google - ics Calendar file

CPV - Saturday - 13:00-13:15 PDT

Title: CPV: Intro to Cyphers
When: Saturday, Aug 10, 13:00 - 13:15 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Are you getting stuck on solving ciphers in challenges? Not sure who or what Caesar is? What is "polyalphabetic" or "transposition"? Is this even relevant to modern day cryptography? Come on over for the Intro to Ciphers talk! Talk time: 5-15 minutes

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: CrackMeIfYouCan
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05 - Map

Description:

Zoogleta has been scheming to corporatize and enshittify the Internet through regulatory capture, squashing indy devs, and commodifying users.

You've been contacted by journalists and whistleblowers who need help sifting through some big dumps of encrypted data and password hashes.

Help them so they can publish the smoking gun, crash Zoogleta's stock price, and get their leadership and the corrupt politicians they own arrested by exposing their internal dirt, for great justice.

Time is of the essence! You will have 48 hours to crack as many files and hashes as possible.

Open to all; preregistration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at https://contest.korelogic.com/ , and the Password Village at https://passwordvillage.org/

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-10:59 PDT

Title: CrackMeIfYouCan
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05 - Map

Description:

Zoogleta has been scheming to corporatize and enshittify the Internet through regulatory capture, squashing indy devs, and commodifying users.

You've been contacted by journalists and whistleblowers who need help sifting through some big dumps of encrypted data and password hashes.

Help them so they can publish the smoking gun, crash Zoogleta's stock price, and get their leadership and the corrupt politicians they own arrested by exposing their internal dirt, for great justice.

Time is of the essence! You will have 48 hours to crack as many files and hashes as possible.

Open to all; preregistration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at https://contest.korelogic.com/ , and the Password Village at https://passwordvillage.org/

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: CrackMeIfYouCan
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05 - Map

Description:

Zoogleta has been scheming to corporatize and enshittify the Internet through regulatory capture, squashing indy devs, and commodifying users.

You've been contacted by journalists and whistleblowers who need help sifting through some big dumps of encrypted data and password hashes.

Help them so they can publish the smoking gun, crash Zoogleta's stock price, and get their leadership and the corrupt politicians they own arrested by exposing their internal dirt, for great justice.

Time is of the essence! You will have 48 hours to crack as many files and hashes as possible.

Open to all; preregistration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at https://contest.korelogic.com/ , and the Password Village at https://passwordvillage.org/

Return to Index - Add to Google - ics Calendar file

CON - Friday - 11:00-11:59 PDT

Title: CrackMeIfYouCan
When: Friday, Aug 9, 11:00 - 11:59 PDT
Where: Virtual

Description:

Zoogleta has been scheming to corporatize and enshittify the Internet through regulatory capture, squashing indy devs, and commodifying users.

You've been contacted by journalists and whistleblowers who need help sifting through some big dumps of encrypted data and password hashes.

Help them so they can publish the smoking gun, crash Zoogleta's stock price, and get their leadership and the corrupt politicians they own arrested by exposing their internal dirt, for great justice.

Time is of the essence! You will have 48 hours to crack as many files and hashes as possible.

Open to all; preregistration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at https://contest.korelogic.com/ , and the Password Village at https://passwordvillage.org/

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-14:59 PDT

Title: Crash and Compile - Qualifications
When: Friday, Aug 9, 10:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 4/Contest Area - Map

Description:

What happens when you take an ACM style programming contest, smash it head long into a drinking game, throw in a mix of our most distracting helpers, then shove the resulting chaos incarnate onto a stage? You get the contest known as Crash and Compile.

Teams are given programming challenges and have to solve them with code. If your code fails to compile? Take a drink. Segfault? Take a drink. Did your code fail to produce the correct answer when you ran it? Take a drink. We set you against the clock and the other teams. And because our "Team Distraction" think watching people simply code is boring, they have taken it upon themselves to be creative in hindering you from programming, much to the enjoyment of the audience. At the end of the night, one team will have proven their ability, and walk away with the coveted Crash and Compile trophy.

Crash and Compile is looking for the top programmers to test their skills in our contest. Do you have the problem solving and programming ability to complete our challenges? More importantly can you do so with style that sets your team ahead of the others? We encourage you to try your hand at the Crash and Compile qualifiers. Gather your team and see if you have the coding chops to secure your place as one of the top teams to move on to the main contest event.

Qualifications for Crash and Compile will take place 10:00 to 15:00. Come see us in contest area West Hall 4, or if you are excited to get started, qualifying can be completed from anywhere, as it takes place online at https://crashandcompile.org. You need a two hour block of time to complete the qualifying round. Points are awarded based on time to complete and problem difficulty.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 16:00-18:59 PDT

Title: Crash and Compile
When: Saturday, Aug 10, 16:00 - 18:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

In-person contest Friday: 10:00 to 15:00, Qualifications Contest Area Saturday: 16:00 - 19:00 Contest Stage

What happens when you take an ACM style programming contest, smash it head long into a drinking game, throw in a mix of our most distracting helpers, then shove the resulting chaos incarnate onto a stage? You get the contest known as Crash and Compile.

Teams are given programming challenges and have to solve them with code. If your code fails to compile? Take a drink. Segfault? Take a drink. Did your code fail to produce the correct answer when you ran it? Take a drink. We set you against the clock and the other teams. And because our "Team Distraction" think watching people simply code is boring, they have taken it upon themselves to be creative in hindering you from programming, much to the enjoyment of the audience. At the end of the night, one team will have proven their ability, and walk away with the coveted Crash and Compile trophy.

Crash and Compile is looking for the top programmers to test their skills in our contest. Do you have the problem solving and programming ability to complete our challenges? More importantly can you do so with style that sets your team ahead of the others? We encourage you to try your hand at the Crash and Compile qualifiers. Gather your team and see if you have the coding chops to secure your place as one of the top teams to move on to the main contest event.

Qualifications for Crash and Compile will take place 10:00 to 15:00. Come see us in contest area West Hall 4, or if you are excited to get started, qualifying can be completed from anywhere, as it takes place online at https://crashandcompile.org. You need a two hour block of time to complete the qualifying round. Points are awarded based on time to complete and problem difficulty.

Return to Index - Add to Google - ics Calendar file

CLV - Sunday - 11:10-11:45 PDT

Title: Creating Azure Policy Compliant Backdoor
When: Sunday, Aug 11, 11:10 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Azure Policy is a built-on service that helps creating security and compliance policies to enforce organizational standards in the cloud environment. It evaluates resources by comparing the properties of the resources and with the help of remediation tasks, it can fix or remediate any issues with those resources. Have you ever wondered if you could abuse or bend these policies? Can you do more than just listing the storage accounts with public access and not be in the logs? How about creating a backdoor?

In this talk I will answer these questions by talking about what Azure Policy is, how to write one, what the logs contain, what permission you need, what does resource enumeration could look like etc. At the end I will present a proof-of-concept solution to bend the Azure Policy and create a backdoor account in Azure.

SpeakerBio: Viktor Gazdag

Viktor Gazdag has worked as pentester and security consultant for 9 years, lead cloud research working group and M365 capability service. He has reported numerous vulnerabilities in products and plugins from companies such as Oracle, SAP, Atlassian, Jenkins, CloudBees Jenkins, JetBrains, Sonatype. He gave talks about CI/CD security at DevOps World, Black Hat USA, DefCon and DoD CyberDT XSWG. He holds multiple AWS/Azure/GCP, Infra as Code, DevOps and Hacking certs and Jenkins Security MVP award.

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 17:00-17:59 PDT

Title: CTI is Dead, Long Live CTI: Reassessing Blue Team's Squishiest Value Proposition (BTV Panel)
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

CTI (Cyber Threat Intelligence) is hard, dumb, silly, a co$t center, a chaotic mess, nonsensical magic…dead. Let this panel change your mind that it is more than a threat feed or a too-long-to-read report. Where is the value?!?!?!

Join us while we navigate the squishy love-hate relationship with CTI. Can we deliver on showing there is value to CTI? You be the judge...

Speakers: Aurora Johnson,Ben Goerz,Ch33r10,Jamie Williams,Rebecca Ford

SpeakerBio: Aurora Johnson, SpyCloud Labs

Aurora Johnson is an information security researcher and cybersecurity policy expert with experience working in both the public and private sectors. She is currently a member of the security research team at SpyCloud Labs and manages SpyCloud's responsible disclosure program. Prior to joining SpyCloud, Aurora served as a Senior Analyst for the Cybersecurity and Infrastructure Security Agency (CISA) and co-founded the agency's Pre-Ransomware Notification Initiative (PRNI). Aurora participates in a range of volunteer and public-private initiatives to track and disrupt the cybercriminal ecosystem; she was a recipient of the President's Volunteer Service Award in 2023 for work with the U.S. government against cyber security threats.

SpeakerBio: Ben Goerz

Ben Goerz is an "InfoSec Janitor" who finds equal comfort in Bash commands and Excel budgets.

Ben has more than a decade of experience building teams in Blue, Red & Purple Team, Threat Intel & Hunting, AppSec, Vulnerability & Attack Surface Management, and Security Consulting. He is a Director at Royal Caribbean Group, and previously held leadership roles in Fortune 500 companies, security vendors, and startups.

After work, Ben can be found tinkering on Raspberry Pi projects with his kids or dropping spicy memes in trust groups.

SpeakerBio: Ch33r10

Ch33r10 (Dr. Xena Olsen) is a cybersecurity professional focused on cyber threat intelligence at a Fortune 100 Financial Services company. She enjoys discussing all things cyber threat intelligence and can be found in various threat intelligence sharing groups, such as Curated Intel. She is a SANS Women's Academy graduate with 8 GIAC certifications, an MBA in IT Management, and a doctorate in Cybersecurity with a focus in Enterprise Purple Teaming.

SpeakerBio: Jamie Williams, Palo Alto Networks Unit 42

Jamie is currently a threat researcher at Palo Alto Networks Unit 42, where he helps lead tailored, tactical and strategic intelligence deliveries. Prior to Unit 42, Jamie was a cyber operations engineer for the MITRE Corporation where he led development of MITRE ATT&CK® for Enterprise and worked with amazing people on various other exciting efforts involving security operations and research, mostly focused on adversary emulation and behavior-based detections.

SpeakerBio: Rebecca Ford

Rebecca founded and leads the cyber threat intelligence program at a major media and entertainment company. She has over 18+ years of experience in cybersecurity and cyber threat intel working for the U.S. government as an APAC analyst with a focus on North Korean cyber activity.

When Rebecca isn't working, she and her husband like playing with their French Bulldog FiFi and volunteering her time speaking at veterans organizations to help service members and their spouses/partners transition from military life to the private sector.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: CubeSat Simulator
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

The AMSAT Ground Control and CubeSat simulator emulates how satellite communications are used. Ground control communicates via UHF to the cubesat.

SpeakerBio: AMSAT

No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: CubeSat Simulator
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

The AMSAT Ground Control and CubeSat simulator emulates how satellite communications are used. Ground control communicates via UHF to the cubesat.

SpeakerBio: AMSAT

No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: CubeSat Simulator
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

The AMSAT Ground Control and CubeSat simulator emulates how satellite communications are used. Ground control communicates via UHF to the cubesat.

SpeakerBio: AMSAT

No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 10:00-11:45 PDT

Title: CULT OF THE DEAD COW & Friends Present: Prime Cuts from Hacker History - 40 Years of 31337
When: Saturday, Aug 10, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

The year is 1984… Ronald Reagan is President, it is a “New Mourning in America.” In Texas, a small cabal of malcontents meet in an abandoned slaughterhouse, decorated with heavy metal band posters, satanic iconography, and, most ominously, the skull of a DEAD COW… As pirated copies of speedmetal and punk music play in the background, these erstwhile revolutionaries speak of their disillusion with The Way Things Are, and their obsession with their new computers. All over America, teens were waking to not just the typical dissatisfaction of adolescence, but the awareness that via these new modes of communication and interaction, they could meet like-minded others, have some illicit fun, and maybe, just maybe, change the goddamn world.

1984 wasn’t the beginning of hacking, but brought perhaps the first real blossoming of the culture. The spread of the personal computer, and the modem, brought the birth of not just cDc, but the Legion of Doom, and 2600 Magazine. 1985 would bring Phrack Magazine, and a true explosion in the written culture, with t-files becoming the currency of the Truly Elite. In this session, members of cDc, 2600, LoD, MoD, and r00t will talk about what made them hackers and phreaks, swap stories, and answer questions posed by Prof. Walter Scheirer of the University of Notre Dame and audience Q&A.

Speakers: Deth Veggie,Walter J. Scheirer,Patrick “Lord Digital” Kroupa,John Threat,Emmanuel Goldstein,X,TommydCat

SpeakerBio: Deth Veggie

cDc Minister of Propaganda, Archaeologist, Gadabout. Cultee since 1990, r00t since 1995, K-rad since birth.

SpeakerBio: Walter J. Scheirer

Dennis O. Doughty Collegiate Professor of Engineering at the University of Notre Dame. Author of A History of Fake Things on the Internet (Stanford University Press, 2023)

SpeakerBio: Patrick “Lord Digital” Kroupa

Member Legion of Doom (LoD) & cDc, Co-founder Mindvox

SpeakerBio: John Threat

world renowned hacker, futurist, security advisor, artist, professor, and writer/director. Wired Magazine Cover, 60 Minutes, MoD, 8lgm, & r00t

SpeakerBio: Emmanuel Goldstein

Editor & Publisher 2600 Magazine, HOPE Conference coordinator, host of WBAI's "Off The Hook”

SpeakerBio: X

Hacker/Vulnerability Archivist, r00t, creator of one of the earliest and longest running vulnerability databases in the World.

SpeakerBio: TommydCat

Technology Generalist and Oldskool Denizen of the Computer Underground, from the 80s onward, TdC's ridden the wave from the days of dumping G-PHilez on AEs to dumping DBs in S3s.

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 15:00-15:25 PDT

Title: Current EW techniques
When: Saturday, Aug 10, 15:00 - 15:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

GPS Jamming and GPS Spoofing. Vulnerabilities in typical GPS receivers Some simple mods that can help Direction finding on GPS Jammers. Overview of DF techniques Artillery Radars Jam resistance HF Communications. (Basically the same thing the Germans did when they were in the Ukraine!)

SpeakerBio: Kent Britain

Kent has an extensive background in Electronic Warfare and will be discussing some of the techniques being used in the Russia-Ukraine conflict

Return to Index - Add to Google - ics Calendar file

DC - Friday - 11:30-12:30 PDT

Title: Custom, cheap, easy, and safe badges - without starting from scratch
When: Friday, Aug 9, 11:30 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Electronic conference badges are cool and everything, but they're A LOT of time, money, and effort including but not limited to hardware, software and art design, testing, manufacturing, testing, provisioning, and repairing.

I'll share OpenTaxus, a relatively simple, cheap, mass-producible, and open-source badge design. We'll start out by looking at and understanding the design and implementation, highlighting the areas worth customizing (and which to leave as-s). I'll do a walkthrough of a few changes to customize the design - in KiCAD for hardware changes, and in CircuitPython for software changes.

We'll wrap up with some discussion of how to handle cost reduction to fit in a certain budget, manage badge logistics for events of different sizes, and warn about some of the many pitfalls that electronic badges suffer. You should walk away with the ability to customize a badge to be mass produced for your own event.

SpeakerBio: Joe "securelyfitz" FitzPatrick, Instructor and Researcher at SecuringHardware.com

Joe FitzPatrick (@securelyfitz) is an Instructor and Researcher at SecuringHardware.com. Joe started his career working on low-level silicon debug, security validation, and penetration testing of CPUS, SOCs, and microcontrollers. He founded SecuringHardware.com and has spent decades developing and leading hardware security-related training, instructing hundreds of security researchers, pen-testers, hardware validators worldwide. When not teaching classes on applied physical attacks, Joe is busy developing new course content or working on contributions to the NSA Playset and other misdirected hardware projects, which he regularly presents at all sorts of fun conferences.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Cyber Defender - The Game
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-C - Map

Description:

Various cyber tools and techniques have been utilized based on information from past attacks. Game players will learn about different cyber security frameworks, cyber-attack processes, and how they can use utilised in a fun way. The game is built to teach key cyber terms, theory and apply techniques based on real-world scenarios.

As a player, you are part of a Global Cyber Protection Team (GCPT) assigned to the mission to prevent various attacks on critical infrastructure. Your task is to use the available information that your team has at your disposal to stop the adversary from achieving their objective.

Players will find themselves in a variety of future scenarios based on a specific industry/sector focus e.g. manufacturing, utilities, defense, finance. The task will be to defend each individual network/system to govern, identify, detect, respond and recover against abnormal/suspicious activities on the network. You will be working against a global hacker network who are threatening to disrupt the overall operations of global critical infrastructure sites for their own nefarious means.

Your team must protect various networks/systems as part of a global environment. If 5 or more systems are compromised and deactivated, the hacker network successfully disabled the global environment and can assume control of the entire environment. It is your mission to protect the environment and ensure the availability of the global system.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Cyber Defender - The Game
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-C - Map

Description:

Various cyber tools and techniques have been utilized based on information from past attacks. Game players will learn about different cyber security frameworks, cyber-attack processes, and how they can use utilised in a fun way. The game is built to teach key cyber terms, theory and apply techniques based on real-world scenarios.

As a player, you are part of a Global Cyber Protection Team (GCPT) assigned to the mission to prevent various attacks on critical infrastructure. Your task is to use the available information that your team has at your disposal to stop the adversary from achieving their objective.

Players will find themselves in a variety of future scenarios based on a specific industry/sector focus e.g. manufacturing, utilities, defense, finance. The task will be to defend each individual network/system to govern, identify, detect, respond and recover against abnormal/suspicious activities on the network. You will be working against a global hacker network who are threatening to disrupt the overall operations of global critical infrastructure sites for their own nefarious means.

Your team must protect various networks/systems as part of a global environment. If 5 or more systems are compromised and deactivated, the hacker network successfully disabled the global environment and can assume control of the entire environment. It is your mission to protect the environment and ensure the availability of the global system.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Cyber Defender - The Game
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-C - Map

Description:

Various cyber tools and techniques have been utilized based on information from past attacks. Game players will learn about different cyber security frameworks, cyber-attack processes, and how they can use utilised in a fun way. The game is built to teach key cyber terms, theory and apply techniques based on real-world scenarios.

As a player, you are part of a Global Cyber Protection Team (GCPT) assigned to the mission to prevent various attacks on critical infrastructure. Your task is to use the available information that your team has at your disposal to stop the adversary from achieving their objective.

Players will find themselves in a variety of future scenarios based on a specific industry/sector focus e.g. manufacturing, utilities, defense, finance. The task will be to defend each individual network/system to govern, identify, detect, respond and recover against abnormal/suspicious activities on the network. You will be working against a global hacker network who are threatening to disrupt the overall operations of global critical infrastructure sites for their own nefarious means.

Your team must protect various networks/systems as part of a global environment. If 5 or more systems are compromised and deactivated, the hacker network successfully disabled the global environment and can assume control of the entire environment. It is your mission to protect the environment and ensure the availability of the global system.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 13:30-13:55 PDT

Title: Cyber Informed Engineering for Critical Infrastructure
When: Friday, Aug 9, 13:30 - 13:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

In an era where critical infrastructure faces unprecedented cyber threats, Cyber Informed Engineering (CIE) emerges as a pivotal strategy to safeguard essential services. This talk delves into the significance of integrating CIE into both existing installations and new builds, highlighting its transformative impact on enhancing security and resilience. Attendees will gain insights into practical applications of CIE, exploring use cases that demonstrate its efficacy in retrofitting legacy systems and embedding robust cybersecurity measures in new projects. Additionally, we'll discuss how CIE serves as a powerful tool for comprehensively understanding and optimizing business processes, ultimately driving more secure and efficient operations. Join us to uncover the essential role of Cyber Informed Engineering in fortifying our critical infrastructure against evolving cyber threats.

SpeakerBio: Aaron Crow

Aaron Crow has over two decades of experience in cybersecurity, focusing on the power utility and operational technology (OT) sectors. At Luminant (Vistra), he managed OT cybersecurity for over 40 power generation sites, including a nuclear plant. Aaron has worked as a consultant, where he led OT cybersecurity programs and influenced product development and as CTO where he helped drive product and direction focusing OT cybersecurity. He hosts the "PrOTect IT All" podcast, sharing insights from industry experts, and advises Building Cyber Security, helping improve security practices in building management systems. Aaron's extensive career highlights his deep understanding of the challenges in securing critical infrastructure.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 10:00-11:45 PDT

Title: Cyber Security Transformation Chef (CSTC)
When: Saturday, Aug 10, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W307 - Map

Description:

Imagine GCHQ's CyberChef integrated in BurpSuite with live modification of requests at your fingertips. That's exactly what we had in mind when we built the Cyber Security Transformation Chef (CSTC) a few years ago. The CSTC is an extension to the popular BurpSuite Proxy built for experts working with web applications. It enables users to define recipes that are applied to outgoing or incoming HTTP requests/responses automatically. Whatever quirks and specialties an application might challenge you with during an assessment, the CSTC has you covered. Furthermore, it allows to quickly apply custom formatting to a chosen message, if a more detailed analysis is needed. After the initial release the CSTC is finally back! It contains new features and improvements such as many new operations to be used in recipes, inclusion of community requested features and a refactoring of the codebase. Alongside the CTSC we will launch a new public repository with recipes we found useful in our experience as penetration testers and of course open for contribution by the community. This helps the community to solve common challenges and getting started working with the CSTC.

Speakers: Florian Haag,Matthias Göhring

SpeakerBio: Florian Haag, Managing Security Consultant at usd AG

Florian Haag is a managing security consultant at usd AG with experience in penetration testing, software security assessments as well as code reviews. He is specialized in penetration tests of thick client applications, leveraging his background in software development to reverse engineer proprietary client applications and network protocols. In addition, he maintains several open source tools for web application pentesting presented at international conferences like BlackHat and DEF CON.

SpeakerBio: Matthias Göhring, Security Consultant and Penetration Tester at usd AG

Matthias Göhring is security consultant and penetration tester at usd AG, an information security company based in Germany with the mission #moresecurity. He is Head of usd HeroLab, the division of usd specialized in technical security assessments. In addition, he holds lectures at Technical University Darmstadt and University of Applied Sciences Darmstadt on ethical hacking and penetration testing. In previous scientific work, he focused on network and communication security as well as software security.

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 16:00-17:59 PDT

Title: Cyberjutsu Path to a Digital Martial Art
When: Saturday, Aug 10, 16:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

Cyberjūtsu is a new way to teach cybersecurity inspired from martial arts trainings. It is an educational way which allows everyone (novice to expert) to practice together and improve themselves in cybersecurity through confrontation. It follows budō (judo, jujitsu, karate...) principles and ethical code. The goal is to reach "maximum-efficient use of computer" in a "mutual benefit" of a human confrontation. It's a digital martial art fight e-sport using linux shell. No matter your technical background—from 10-year-olds to technical experts like pentesters and red/blue teamers—this workshop is designed for you. The only prerequisite is basic reading, writing, and counting knowledge. Experience real live adversary sparring and see how even those with less knowledge can outmaneuver more experienced participants. Join us for an interactive session with 14 players participating and others welcome to watch. Enhance your cybersecurity skills through collaborative and practical exercises.

Speakers: Alexandre CABROL PERALES,Quentin Fraty,Alaric Becker

SpeakerBio: Alexandre CABROL PERALES, President of NPO multi-country WOCSA, Director of Managed Detection & Response at Sopra Steria, Teacher at French University Cyber Master

President of WOCSA France, Cyberjutsu Project Leader for WOCSA Head of Managed Detection and Response Services at Sopra Steria Cybersecurity External Professor at Cybersecurity Master (SSIR) for Science University of Toulouse, France. 1st dan Judo Jujitsu

SpeakerBio: Quentin Fraty, Threat Intelligence Analyst and Reverse at Sopra Steria

I'm passionate about cybersecurity: since I joined my engineering school in 2021, I started organizing cybersecurity workshops for WOCSA. Attendees range from experiences pentesters to curious teenagers that simply want to have some fun, but I believe that we can all learn something from eachother.

SpeakerBio: Alaric Becker, SOC Analyst and Threat Hunter at Sopra Steria

WOCS'HACK Project Leader for WOCSA France. Security Operation Center Analyst at Sopra Steria Cybersecurity. 3rd dan Judo Jujitsu

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 11:30-12:30 PDT

Title: Cybersecurity for Emerging Tech (panelists would include researchers or industry executives in emerging tech categories, like space, OT, hardware like drones, etc)
When: Saturday, Aug 10, 11:30 - 12:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:
SpeakerBio: Paulino Calderon
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 15:00-15:45 PDT

Title: Cybersecurity for Veterans: Bridging the Gap from Military to Civilian Careers
When: Saturday, Aug 10, 15:00 - 15:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:
SpeakerBio: Matt James
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 17:00-17:59 PDT

Title: Cybersecurity Overview over LATAM- Skills, Challenges, Knowledge, Perspectives
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

En este panel vamos a revisar desde la perspectiva de diferentes profesionales los desafios de hacer ciberseguridad en LATAM, los conocimientos o falta de ellos que se pueden evidenciar en diferentes sectores y las necesidades de habilidades existentes actuales en la region para mantener un ecosistema protegido de las amenazas que deben ser enfrentadas a diario

Speakers: Leonardo Pigñer,Katherina Canales,Victor Santos

SpeakerBio: Leonardo Pigñer, CEO y Co-Founder Ekoparty

Leo Pigñer es co-fundador y CEO de Ekoparty, la conferencia hacker más importante de Latinoamérica. Con más de 20 años en la industria de ciberseguridad, Pigñer tambien es co-fundador de BASE4 Security, empresa proveedora de servicios de ciberseguridad en Latinoamérica y España.

SpeakerBio: Katherina Canales, Directora Ejecutiva de la Corporación de Ciberseguridad Minera

Actualmente es Directora Ejecutiva de la Corporación de Ciberseguridad Minera. Katherina es ex Directora Operacional del CSIRT de gobierno de Chile, experta en estrategias de ciberseguridad, con especial énfasis en políticas públicas, equipos de respuesta ante incidentes de seguridad informática y concientización. Reconocida por la academia, la industria e internacionalmente como mujer influyente en ciberseguridad

SpeakerBio: Victor Santos, CEO da Clavis Segurança da Informação
No BIO available

Return to Index - Add to Google - ics Calendar file

PLV - Friday - 16:00-16:30 PDT

Title: Cybersecurity Schoolhouse Rock
When: Friday, Aug 9, 16:00 - 16:30 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Almost since the internet was made widely available to the general public, average technology users have fallen prey to threats from malicious spam, malware, phishing, smishing, scams, fraud, and ransomware. In most of the US, primary and secondary education (in the US, comprising kindergarten through 12th grade) now incorporate computing technology as an integral part of the classroom, and some families introduce computing platforms to children in their toddler and preschool years. Despite our society's growing dependence on computing technology in the world of education, there remain no national standards or curricula for the teaching of data privacy or information security principles. This disconnect sets future generations up for failure, and a continuation of a cycle of ignorance that perpetuates cybercrime victimization. This presentation makes the case that schools must adopt and incorporate concepts of data privacy, information security, defense against fraud and phishing, and internet safety, in age-appropriate ways, into lesson plans at all grade levels. Further, school districts and independent schools must take steps to protect themselves from the threat of ransomware, data breaches, and other forms of criminal activity.

SpeakerBio: Avi McGrady

Avi McGrady is a recently graduated student of New Vista High School in Boulder, Colorado. He prepared the research and work for this presentation as a part of a culminating project in his senior year, and presented a report to the Boulder Valley School District board as part of this work toward his graduation requirements. Avi is an enthusiastic student of computer science and information security and hopes to work in the field after he graduates. He will attend Rensselaer Polytechnic Institute as an undergraduate freshman in the fall of 2024. His passion has led him to attend and volunteer for two infosec conferences, RMISC and Bsides in Boulder, and he will be leaning further into his outreach as he begins college and starting his career.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 06:00-06:59 PDT

Title: CycleOverride DEF CON Bike Ride
When: Friday, Aug 9, 06:00 - 06:59 PDT
Where: Other / See Description

Description:

At 6am on Friday, the @cycle_override crew will be hosting the 13th DEF CON Bikeride. We'll meet at a local bikeshop, get some rental bicycles, and about 7am will make the ride out to Red Rocks. It's about a 15 mile ride, all downhill on the return journey. So, if you are crazy enough to join us, get some water, and head over to cycleoverride.org for more info. See you at 6am Friday! @jp_bourget @gdead @heidishmoo.

Return to Index - Add to Google - ics Calendar file

Title: D0N0H4RM: Cyber STEM Storytime
When: Saturday, Aug 10, 15:30 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Speakers: Nitin Natarajan,Christian Dameff,Andrew Carney,Matt Hazelett,Erika Cheung

SpeakerBio: Nitin Natarajan, Deputy Director at Cybersecurity and Infrastructure Security Agency (CISA)

Nitin Natarajan was appointed to serve as the Deputy Director for the Cybersecurity and Infrastructure Security Agency (CISA) on February 16, 2021. Prior to joining CISA, Natarajan served in a variety of public and private sector positions spanning over 30 years. Most recently he served as an executive with consulting firms within the National Capital Region, providing subject matter expertise on a variety of topics, including cybersecurity, homeland and national security, critical infrastructure protection, environmental emergency management, continuity of operations, and health security matters. Natarajan also held a number of federal government roles to include Deputy Assistant Administrator at the U.S. Environmental Protection Agency, the Director of Critical Infrastructure Policy at the White House/National Security Council, and as a Director at the U.S. Health and Human Services overseeing healthcare and public health programs. Prior to serving in the federal government, Natarajan served in positions at the state/local government level and served as a hospital administrator in New York. At the beginning of his career, Natarajan spent 13 years as a first responder in New York, which included service as a flight paramedic. He was the Commander of a federal medical response team, based in New York, and has extensive experience deploying to natural and man-made disasters throughout the nation. He holds an undergraduate degree from the State University of New York and a graduate degree from the United States Naval Postgraduate School.

SpeakerBio: Christian Dameff, Emergency PhysicianMD

Dr. Christian Dameff is an Emergency Physician, Clinical Informaticist, and researcher. Published clinical works include post cardiac arrest care including therapeutic hypothermia, novel drug targets for acute myocardial infarction patients, ventricular fibrillation waveform analysis, cardiopulmonary resuscitation (CPR) quality and optimization, dispatch assisted CPR, teletoxicology, clinical applications of wearables, and electronic health records.

Dr. Dameff is also a hacker and security researcher interested in the intersection of healthcare, patient safety, and cybersecurity. He has spoken at some of the world's most prominent hacker forums including DEFCON, RSA, Blackhat, Derbycon, BSides: Las Vegas, and is one of the cofounders of the CyberMed Summit, a novel multidisciplinary conference with emphasis on medical device and infrastructure cybersecurity. Published cybersecurity topics include hacking 911 systems, HL7 messaging vulnerabilities, and malware.

SpeakerBio: Andrew Carney, Program Manager at Advanced Research Projects Agency for Health (ARPA-H)

Andrew Carney joined ARPA-H in July 2023 from HSBC's Cybersecurity Science and Analytics group, where he worked as a principal researcher. He has over 15 years of experience in software and hardware vulnerability research, technical education and training, and management of research and development teams.

In addition to his role as program manager with ARPA-H, Carney holds a joint program manager appointment with the Defense Advanced Research Projects Agency (DARPA) for the AI Cyber Challenge (AIxCC), a competition focused on securing software in critical infrastructure. Before HSBC, Carney was a technical advisor and contractor for the Defense Advanced Research Projects Agency (DARPA). At DARPA, he supported research efforts focused on reverse engineering, program analysis, human-machine teaming, and automated program repair. Throughout his career, Carney has been involved in competitive hacking (called Capture the Flag, or CTF) as both a player and a competition organizer. He holds a master's degree in computer science from The Johns Hopkins University.

SpeakerBio: Matt Hazelett, Program Director for the Cybersecurity Focal Point Program in the Office of Product Evaluation and Quality (OPEQ) at FDA

I coordinate across the Center for Devices and Radiological Health (CDRH) at FDA on medical device cybersecurity policy development, vulnerability and incident response, and policy implementation across the total product lifecycle (TPLC).

I have led and oversee the implementation of Section 524B, Ensuring Cybersecurity of Devices, of the Food, Drug, and Cosmetic (FD&C) Act and the FDA guidance, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. This includes making available training for over 1000 review staff and managers, developing submission support resources (eSTAR Template and help text), developing support resources for review staff, and answering policy questions.

Also, as the Program Director for the Cybersecurity Focal Point Program in the Office of Product Evaluation and Quality (OPEQ), I work to build reviewer subject matter expertise in medical device cybersecurity as well as build and maintain consistency across the review offices and the TPLC.

SpeakerBio: Erika Cheung, Executive Director at Ethics in Entrepreneurship

Currently, the Executive Director of Ethics in Entrepreneurship, a non-profit whose mission is to foster ethical questioning, culture, and systems in startups and startup ecosystems. We provide programs catered to workers, investors, and founders.

Erika is an advisor to several family offices, venture capital firms, and governmental investment programs focused on healthcare, biosciences, and biotechnology companies. She invests a portion of her time building cross-border networks between the US and the Asia Pacific region to facilitate the growth of companies operating in emerging markets.

Her first job out of college was working for Theranos, where she subsequently was one of the critical whistleblowers reporting the fraud case to regulators preventing the company from providing false lab results to patients. The Theranos scandal has been extensively covered in the media. She's working towards obtaining her ACFE-certified fraud examiner's license to educate others on fraud prevention strategies and develop programs to protect business stakeholders from high-risk ventures. She is also an advisor to several whistleblower advocacy organizations to support individuals who may be retaliated against while reporting misconduct.

She is passionate about innovation ecosystem building, development, economic mobility, affordable healthcare, and public-interest technology projects. She is an avid mixed martial artist in her free time and hopes to support efforts that leverage martial arts to empower trauma survivors

---

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 13:30-14:30 PDT

Title: DarkGate: Cazando a la amenaza y exponiendo su infraestructura
When: Saturday, Aug 10, 13:30 - 14:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Con el continuo crecimiento de las amenazas en el ciberespacio y la escasez de guías efectivas para analizar, detectar y estar un paso adelante de los adversarios, expondremos durante nuestra plática cómo, a través de la inteligencia de ciber-amenazas y el análisis de malware, podemos desmantelar la infraestructura de los atacantes y anticiparnos a sus objetivos. Utilizaremos técnicas de Threat Hunting para demostrar cómo detectar comportamientos anómalos dentro de una red y proporcionar a los asistentes las herramientas necesarias, incluyendo Indicadores de Compromiso (IoCs), Tácticas, Técnicas y Procedimientos (TTPs), e infraestructura no detectada (Hunting Infrastructure), para enfrentar la actividad maliciosa del malware conocido como DarkGate.

SpeakerBio: Nestor Sánchez, Cyber Threat Hunter at GNP

Nestor Sánchez es un profesional con 6 años de experiencia en el campo de la ciberseguridad principalmente en Cyber Threat Hunting destacando en la detección temprana de amenazas, el analisis y la mitigación de distiantos adversarios que afectan al sector financiero/asegurador, asi como el desarrollo de inteligencia para un mejor postura de seguridad antes las distintas amenazas que se encuentran en el mundo digital.

Nestor Sánchez ha colobaroado y se ha desempñeado en distintas areas de la ciberseguridad, como son: Cyber threat intelligence, Incidente Response y Digital forensics, desempeñando diversas tareas que han ayudado a mitigar y detectar distintos actores amenaza asi como mejorar la postura de seguridad seguridad de las organizaciones.

Nestor es egresado de la facultad de estudios superiores aragon (UNAM) asi como colaborador del laboratorio de seguridad de la misma, actualmente cuenta con 3 certificaciones dos emitidad por el SANS y 1 emitada por eLearn Security (INE) que son: GCFA - Advanced incident response, threat hunting and digital forensics, GCTI - Cyber Threat Intelligence y eCTHP Cyber Threat Hunting Professional

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Darknet-NG
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-D - Map

Description:

Darknet-NG is an Alternate Reality Game (ARG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's final challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site https://darknet-ng.network and join our growing Discord Community!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Darknet-NG
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-D - Map

Description:

Darknet-NG is an Alternate Reality Game (ARG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's final challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site https://darknet-ng.network and join our growing Discord Community!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Darknet-NG
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-D - Map

Description:

Darknet-NG is an Alternate Reality Game (ARG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's final challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site https://darknet-ng.network and join our growing Discord Community!

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Darkstar Badge Challenge
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Collect the clues, solve the puzzles, show off your aerospace knowledge and technical skills to win a limited edition PCB badge.

SpeakerBio: Lockheed Martin
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Darkstar Badge Challenge
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Collect the clues, solve the puzzles, show off your aerospace knowledge and technical skills to win a limited edition PCB badge.

SpeakerBio: Lockheed Martin
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Darkstar Badge Challenge
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Collect the clues, solve the puzzles, show off your aerospace knowledge and technical skills to win a limited edition PCB badge.

SpeakerBio: Lockheed Martin
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: DARPA's Artificial Intelligence Cyber Challenge (AIxCC)
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06 - Map

Description:

DARPA and ARPA-H's Artificial Intelligence Cyber Challenge (AIxCC) will bring together the foremost experts in AI and cybersecurity to safeguard the software critical to all Americans. AIxCC is a two-year competition that asks competitors to design novel AI systems to secure this critical code and will award a cumulative $29.5 million in prizes to Teams with the best systems. In 2024, top teams will be awarded prizes of $2 million each, and will advance to the finals at DEF CON 33. The AIxCC Experience at DEF CON 32 is an immersive and interactive competition environment and educational space to inspire people and organizations to accelerate the development of AI-enabled cyber defenses. Attendees will explore a futuristic city where they can learn all about the competition, the technology, and the power of AI to help secure the software we all depend on.

Registration for AIxCC is no longer open to new contestants. AIxCC Preliminary Events were held March – July 2024.

Semifinalists will be announced here: https://aicyberchallenge.com/

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: DARPA's Artificial Intelligence Cyber Challenge (AIxCC)
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06 - Map

Description:

DARPA and ARPA-H's Artificial Intelligence Cyber Challenge (AIxCC) will bring together the foremost experts in AI and cybersecurity to safeguard the software critical to all Americans. AIxCC is a two-year competition that asks competitors to design novel AI systems to secure this critical code and will award a cumulative $29.5 million in prizes to Teams with the best systems. In 2024, top teams will be awarded prizes of $2 million each, and will advance to the finals at DEF CON 33. The AIxCC Experience at DEF CON 32 is an immersive and interactive competition environment and educational space to inspire people and organizations to accelerate the development of AI-enabled cyber defenses. Attendees will explore a futuristic city where they can learn all about the competition, the technology, and the power of AI to help secure the software we all depend on.

Registration for AIxCC is no longer open to new contestants. AIxCC Preliminary Events were held March – July 2024.

Semifinalists will be announced here: https://aicyberchallenge.com/

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-13:59 PDT

Title: DARPA's Artificial Intelligence Cyber Challenge (AIxCC)
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06 - Map

Description:

DARPA and ARPA-H's Artificial Intelligence Cyber Challenge (AIxCC) will bring together the foremost experts in AI and cybersecurity to safeguard the software critical to all Americans. AIxCC is a two-year competition that asks competitors to design novel AI systems to secure this critical code and will award a cumulative $29.5 million in prizes to Teams with the best systems. In 2024, top teams will be awarded prizes of $2 million each, and will advance to the finals at DEF CON 33. The AIxCC Experience at DEF CON 32 is an immersive and interactive competition environment and educational space to inspire people and organizations to accelerate the development of AI-enabled cyber defenses. Attendees will explore a futuristic city where they can learn all about the competition, the technology, and the power of AI to help secure the software we all depend on.

Registration for AIxCC is no longer open to new contestants. AIxCC Preliminary Events were held March – July 2024.

Semifinalists will be announced here: https://aicyberchallenge.com/

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 14:00-14:30 PDT

Title: Data Brokers and the Threat to Your Privacy
When: Friday, Aug 9, 14:00 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Data brokers, and in particular people-search sites, are a headache for those of us trying to keep our addresses off the internet… and an absolute nightmare for people who are targeted due to their identity, profession, or political beliefs. In this talk, I'll present the results of a collaborative research project by Tall Poppy and Consumer Reports that evaluates paid people-search removal services. I'll also discuss how data brokers harm people, what you can do to protect yourself, why it's so difficult, and what we can do as individuals and at a policy/advocacy level to solve this pernicious privacy problem.

SpeakerBio: Yael Grauer

Yael Grauer is an investigative tech reporter. She currently works at Consumer Reports managing Security Planner, an easy-to-use guide to staying safer online. Yael has over a decade of experience covering privacy and security, digital freedom, hacking, and mass surveillance for various tech publications and has extensively researched the privacy and security (or lack thereof) of VPNs, street-level surveillance, and more. She's been maintaining the Big Ass Data Broker Opt-Out List since 2017.

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 16:00-16:59 PDT

Title: Data On Demand: The challenges of building a privacy focused AI Device
When: Friday, Aug 9, 16:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Building an AI product for the everyday person is challenging - doing it in a privacy focused way is nearly impossible without support from the right people. I'll walk through the techniques we're using at Rabbit to secure customer data and provide people a choice as to where their data goes.

We'll cover the pipelines that - Collect and Manage customer identity after they login to a site - Log, Anonymize, and Process customer voice interactions - Provide "just in time" access to customer data for personalized RAG-like models

As a community, I think we're well within our rights to demand control over the data we provide to companies. This talk aims to provide engineers with a list of ideas on "what right could look like", and general attendees a list of things that are possible, so they know its ok to ask for them.

SpeakerBio: Matt Domko, Head of Security at (in)famous AI Walkie Talkie Manufacturer

Matt Domko is the Head of Security at a (in)famous AI Walkie Talkie Manufacturer. Ex-This, Ex-That, he spends most of his free time tinkering with his lasercutter or 3d printers.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 14:00-15:59 PDT

Title: DC Book Club Discussion
When: Saturday, Aug 10, 14:00 - 15:59 PDT
Where: LVCC West/Floor 2/HallwayCon Lounge past W234 - Map

Description:

A quieter space for those who want to discuss what they are reading, recommend books, and trade books too. We will have a logo themed sticker.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-16:59 PDT

Title: DC Kubernetes Capture the Flag (CTF)
When: Saturday, Aug 10, 10:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-E - Map

Description:

The DEF CON Kubernetes Capture the Flag (CTF) contest features a Kubernetes-based CTF challenge, where teams and individuals can build and test their Kubernetes hacking skills. Each team/individual is given access to a single Kubernetes cluster that contains a set of serial challenges, winning flags and points as they progress. Later flags pose more difficulty, but count for more points.

A scoreboard tracks the teams' current and final scores. In the event of a tie, the first team to achieve the score wins that tie.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-19:59 PDT

Title: DC Kubernetes Capture the Flag (CTF)
When: Friday, Aug 9, 12:00 - 19:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-E - Map

Description:

The DEF CON Kubernetes Capture the Flag (CTF) contest features a Kubernetes-based CTF challenge, where teams and individuals can build and test their Kubernetes hacking skills. Each team/individual is given access to a single Kubernetes cluster that contains a set of serial challenges, winning flags and points as they progress. Later flags pose more difficulty, but count for more points.

A scoreboard tracks the teams' current and final scores. In the event of a tie, the first team to achieve the score wins that tie.

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 19:30-21:59 PDT

Title: DC Next Gen party
When: Saturday, Aug 10, 19:30 - 21:59 PDT
Where: LVCC West/Floor 2/W228 - Map

Description:

Party with DEF CON NextGen. Enjoy some music, and some good conversation with other young DEF CON attendees!

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 10:00-11:50 PDT

Title: DC NextGen / Youth Challenge Area at Red Team Village
When: Sunday, Aug 11, 10:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207 - Map

Description:
SpeakerBio: RTV Staff
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 13:00-16:59 PDT

Title: DC NextGen / Youth Challenge Area at Red Team Village
When: Friday, Aug 9, 13:00 - 16:59 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Ascension - Map

Description:
SpeakerBio: RTV Staff
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 12:00-16:59 PDT

Title: DC NextGen / Youth Challenge Area at Red Team Village
When: Saturday, Aug 10, 12:00 - 16:59 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Ascension - Map

Description:
SpeakerBio: RTV Staff
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: DC's Next Top Threat Model (DCNTTM)
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05-A - Map

Description:

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist.

As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner and crown DEF CON's Next Top Threat Model(er).

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: DC's Next Top Threat Model (DCNTTM)
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05-A - Map

Description:

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist.

As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner and crown DEF CON's Next Top Threat Model(er).

Return to Index - Add to Google - ics Calendar file

DC - Friday - 15:00-15:59 PDT

Title: DC101 Panel
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:
Speakers: Nikita Kronenberg,Drew "aNullValue" Stemen,Grifter,AdaZebra

SpeakerBio: Nikita Kronenberg, Director of Content and Coordination at DEF CON Communications
No BIO available
SpeakerBio: Drew "aNullValue" Stemen, Project Manager at Hacker Tracker
No BIO available
SpeakerBio: Grifter, Contests & Events Lead at DEF CON 32
No BIO available
SpeakerBio: AdaZebra, Head of Hotline at DEF CON 32
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Thursday - 19:00-20:59 PDT

Title: DC702
When: Thursday, Aug 8, 19:00 - 20:59 PDT
Where: LVCC West/Floor 2/W236 - Map

Description:

Join the local DC702 Group in this year's official DEF CON Meetup! The meetup will be casual and include typical meetup activities (e.g., socializing, "challenges," lockpicking, etc.) and maybe a few little surprises. To stay up-to-date, check out dc702.space/dc32-meetup.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 16:00-18:59 PDT

Title: DCG Atlanta (DC404,678,770,470)
When: Friday, Aug 9, 16:00 - 18:59 PDT
Where: LVCC West/Floor 2/W236 - Map

Description:

They say Atlanta is the city too busy to hate, but it also has too much traffic for its widespread hacker fam to get together in a single meetup. So instead, we're meeting up in the desert during DEF CON! The one time of year when intown, northern burbs, south siders, and anyone else connected to DC404's 25+ year legacy can catch up and share stories. Join us and meet your fellow ATL hackers!

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 12:00-12:59 PDT

Title: DCNextGen Awards and Closing Ceremony
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

We will be handing out the CTF Prizes and awards. Must be present to win!

Return to Index - Add to Google - ics Calendar file

DDV - Saturday - 10:00-16:59 PDT

Title: DDV open and accepting drives for duplication
When: Saturday, Aug 10, 10:00 - 16:59 PDT
Where: LVCC West/Floor 2/W225 - Map

Description:

We reopen at 10: 00am and accept drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. Don't forget - some require 8TB drives now. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.

About Us

The Data Duplication Village has all the updated bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for a copy of all the things, we've got what you need to fill up all your storage including a few nice hash tables and all of the DefCon talks. Add to that just about every other security con talk known to hacker-kind! Our village provides a "free-to-you" service of direct access to terabytes of useful data to help build those hacking skills and talk with other storage enthusiasts.

Check the schedule and/or dcddv.org for the most up-to-date information.

How It Works

The DDV provides a core set of drive duplicators and data content options. We accept 8TB and larger drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in your blank SATA3 drives - check them in early - to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO - get those drives in early!

What You Get

We're working on more content right up until the last minute so keep checking on dcddv.org for the latest. This year, we're adding new data to duplicate! Humans will be able to choose from the following data sources for duplication:

- A) Infocon.org Archive - 6TB archive of all the past hacking convention videos that DT could find, built on last years collection and always adding more for your data consuming appetite.
- B) Rainbow tables 1 of 3 - 6TB from freerainbowtables.com, the Lanman, MSQLSHA1, and NTLM hash tables plus freerainbowtables.com tools
- C) Rainbow tables 2 of 3 - 6TB from freerainbowtables.com, the A5/1 GSM, and MD5 tables plus freerainbowtables.com tools
- D) Vx Underground Archive - 8TB archive of the latest papers, samples, and code from Vx Underground
- E) Rainbow tables 3 of 3 - 8TB of New NTLM-9 hash tables and a copy of the Infocon.org mirrors

Return to Index - Add to Google - ics Calendar file

DDV - Friday - 10:00-16:59 PDT

Title: DDV open and accepting drives for duplication
When: Friday, Aug 9, 10:00 - 16:59 PDT
Where: LVCC West/Floor 2/W225 - Map

Description:

We reopen at 10: 00am and accept drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. Don't forget - some require 8TB drives now. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.

About Us

The Data Duplication Village has all the updated bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for a copy of all the things, we've got what you need to fill up all your storage including a few nice hash tables and all of the DefCon talks. Add to that just about every other security con talk known to hacker-kind! Our village provides a "free-to-you" service of direct access to terabytes of useful data to help build those hacking skills and talk with other storage enthusiasts.

Check the schedule and/or dcddv.org for the most up-to-date information.

How It Works

The DDV provides a core set of drive duplicators and data content options. We accept 8TB and larger drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in your blank SATA3 drives - check them in early - to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO - get those drives in early!

What You Get

We're working on more content right up until the last minute so keep checking on dcddv.org for the latest. This year, we're adding new data to duplicate! Humans will be able to choose from the following data sources for duplication:

- A) Infocon.org Archive - 6TB archive of all the past hacking convention videos that DT could find, built on last years collection and always adding more for your data consuming appetite.
- B) Rainbow tables 1 of 3 - 6TB from freerainbowtables.com, the Lanman, MSQLSHA1, and NTLM hash tables plus freerainbowtables.com tools
- C) Rainbow tables 2 of 3 - 6TB from freerainbowtables.com, the A5/1 GSM, and MD5 tables plus freerainbowtables.com tools
- D) Vx Underground Archive - 8TB archive of the latest papers, samples, and code from Vx Underground
- E) Rainbow tables 3 of 3 - 8TB of New NTLM-9 hash tables and a copy of the Infocon.org mirrors

Return to Index - Add to Google - ics Calendar file

DDV - Thursday - 16:00-19:59 PDT

Title: DDV starts accepting drives for duplication
When: Thursday, Aug 8, 16:00 - 19:59 PDT
Where: LVCC West/Floor 2/W225 - Map

Description:

We start taking drives at 4: 00pm local time on Thursday - possibly a little earlier. We'll keep accepting drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. Don't forget - some require 8TB drives now. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.

About Us

The Data Duplication Village has all the updated bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for a copy of all the things, we've got what you need to fill up all your storage including a few nice hash tables and all of the DefCon talks. Add to that just about every other security con talk known to hacker-kind! Our village provides a "free-to-you" service of direct access to terabytes of useful data to help build those hacking skills and talk with other storage enthusiasts.

Check the schedule and/or dcddv.org for the most up-to-date information.

How It Works

The DDV provides a core set of drive duplicators and data content options. We accept 8TB and larger drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in your blank SATA3 drives - check them in early - to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO - get those drives in early!

What You Get

We're working on more content right up until the last minute so keep checking on dcddv.org for the latest. This year, we're adding new data to duplicate! Humans will be able to choose from the following data sources for duplication:

- A) Infocon.org Archive - 6TB archive of all the past hacking convention videos that DT could find, built on last years collection and always adding more for your data consuming appetite.
- B) Rainbow tables 1 of 3 - 6TB from freerainbowtables.com, the Lanman, MSQLSHA1, and NTLM hash tables plus freerainbowtables.com tools
- C) Rainbow tables 2 of 3 - 6TB from freerainbowtables.com, the A5/1 GSM, and MD5 tables plus freerainbowtables.com tools
- D) Vx Underground Archive - 8TB archive of the latest papers, samples, and code from Vx Underground
- E) Rainbow tables 3 of 3 - 8TB of New NTLM-9 hash tables and a copy of the Infocon.org mirrors

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 13:30-13:59 PDT

Title: De Escudo a Espada: Cómo un Antivirus Facilitó el compromiso de una compañía
When: Friday, Aug 9, 13:30 - 13:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

En una actividad de simulación de adversarios, se demostró cómo se puede comprometer una empresa utilizando su antivirus corporativo. Aprovechando las funcionalidades de antivirus de nueva generación, y el compromiso de la consola de administración se logro desplegar un comando y control (C2) en equipos críticos como controladores de dominio. La capacidad del antivirus para comunicarse con subredes críticas y aplicar excepciones a otras herramientas de seguridad facilitó el compromiso total de la red, destacando la necesidad de una gestión y auditoría exhaustivas de estas herramientas.

SpeakerBio: R4v3n Bl4ck, Sr Red Team
Ariel Cruz: OSCP, OSWE, OSWA, OSEP, OWSP, CISSP, CNSS, CEH v10,Autopsy. Más de 10 años generando valor

como red teamer, simulación de adversarios avanzados y pentester. Enfoque en sectores bancarios y

de telecomunicaciones. Cuenta con dominio sobre la metodología MITRE ATT&CK, amplia ejecución

sobre la ejecución de las vulnerabilidades del Top 10 OWASP, así como con diversas certificaciones de

la industria de la ciberseguridad, entre las que puede destacar OffSec Certified Professional, OffSec

Web Expert, OffSec Experienced Penetration Tester.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 11:00-11:45 PDT

Title: Deception & Counter Deception – Defending Yourself in a World Full of Lies
When: Sunday, Aug 11, 11:00 - 11:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

The Internet was supposed to give us access to the world's information, so that people, everywhere, would be able to know the truth. But that's not how things worked out. Instead, we have a digital deception engine of global proportions. Nothing that comes through the screen can be trusted, and even the things that are technically true have been selected, massaged, and amplified in support of someone's messaging strategy.

Deception isn't just about narratives - we see deception at every layer of the network stack, from spoofed electromagnetic signatures, to false flags in malware, to phony personas used to access networks and spread influence. They hide in our blindspots, exploit our biases, and fill our egos while manipulating our perceptions.

How do we decide what is real? This talk examines time-tested maxims that teach the craft of effective deception, and then inverts those offensive principles to provide defensive strategies. We'll explore ways to counter biases, triangulate information sources, detect narratives, and how hackers can build tools that can change the game.

At their best, hackers lift their heads up above the masses to see how the world actually works, not how it purports to work, and then take action to make the world a better place. You'll leave this talk with practical skills to do just that.

Speakers:
Tom "Decius" Cross,Greg Conti

SpeakerBio:
Tom "Decius" Cross, Principal at Kopidion

Tom Cross (aka Decius) is a security researcher known for delivering late night rants at hacker cons. In the early 1990's, he ran BBSs and listservs for the hacker community in the southeast US. He attended the first Defcon in 1993. He is a Principal at Kopidion, and creator of FeedSeer, a news reader for Mastodon. Past security industry roles include cofounder and CTO of Drawbridge Networks, Research Director at Lancope, and Manager of IBM X-Force Advanced Research. He has spoken at numerous conferences, including Black Hat, DEF CON, Phreaknic, HOPE, and B-Sides. He has a BSCMPE from Georgia Tech.

SpeakerBio:
Greg Conti, Principal at Kopidion

Greg Conti is a hacker, maker, and computer scientist. He is Principal at Kopidion, a cyber security training and professional services firm. Greg is a long-time Black Hat trainer where he co-created the Information Operations course. He will also be teaching a new course on Adversarial Thinking at DEF CON Training this year. Formerly he served on the West Point faculty for 16 years and has published approximately 100 articles and papers covering hacking, online privacy, usable security, cyber conflict, and security visualization. Greg is a graduate of West Point, Johns Hopkins, and Georgia Tech

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 16:30-16:59 PDT

Title: Decoding Galah, an LLM Powered Web Honeypot
When: Saturday, Aug 10, 16:30 - 16:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Honeypots are invaluable tools for monitoring internet-wide scans and understanding attackers' techniques. Traditional low-interaction web honeypots use manual methods to emulate various applications or vulnerabilities. Introducing Galah, an LLM-powered web honeypot that mimics diverse applications with a single prompt. This honeypot dynamically crafts relevant HTTP responses, including headers and body content, to various HTTP requests, effectively simulating multiple web applications. In this talk, I will share lessons learned from building and deploying Galah and address two key questions: How do different large language models perform in generating HTTP messages? Does delivering authentic-looking HTTP responses increase attackers' engagement with the honeypot?

SpeakerBio: Adel Karimi, Senior Security Engineer, Detection at Niantic

Adel Karimi is a senior security engineer, detection at Niantic. Before joining Niantic, he served as a lead security engineer at Google and Salesforce, specializing in detecting and responding to "badness." Beyond his day job, Adel, a longtime member of the Honeynet Project, dedicates his expertise to developing open-source projects such as Galah, reflecting his keen interests in honeypots, network fingerprinting, and the broader spectrum of threat detection.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 11:00-12:59 PDT

Title: DEF CON 32 Beard and Mustache Contest
When: Saturday, Aug 10, 11:00 - 12:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

Held every year since DEF CON 19 in 2011 (R.I.P. Riviera), (Except during that COVID thing - but we are not going to talk about that COVID thing), the DEF CON (unofficial) Beard and Mustache Contest highlights the intersection of facial hair and hacker culture.

For 2024 there will be four categories for the competition you may only enter one: - Full beard: Self-explanatory, for the truly bearded. - Partial Beard: For those sporting Van Dykes, Goatees, Mutton Chops, and other partial beard styles. - Mustache only: Judging on the mustache only, even if bearded. Bring your Handlebars, Fu Manchus, or whatever adorns your upper lip. - Freestyle: Anything goes, including fake and creatively adorned beards. Creative women often do well in the Freestyle category.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 16:30-17:15 PDT

Title: DEF CON Academy: Cultivating M4D SK1LLZ In the DEF CON Community
When: Saturday, Aug 10, 16:30 - 17:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

DEF CON is a siren song for the hacker mind. Clever people around the world hear it and are pulled, every year, to Las Vegas. They mass by the tens of thousands, streaming through the halls of DEF CON to watch talks given by absolute legends about incredible escapades, to gaze in wonder as true wizards bend bytes to their will in the CTF room, and to dream about one day reaching to those heights themselves.

Some have the critical combination of grit, perseverance, raw talent, and (let's face it) privilege to push through to those dreams of greatness. But among even the clever and the motivated, it is rare for n00bs to rise to l33tness without support. Some find this support in inspiring classes in college. Others, among friends or mentors. But many don't find it at all, and remain in the hallways, dreaming.

Do you want to leave the hallways and hack the planet? We are hackers, educators, and learners who are creating DEF CON Academy, a concerted effort to maximize hacker potential by providing open, clear, approachable, and inclusive practical resources for budding hackers to transcend and rule cyberspace. Through extensive DEF CON event presence and year-round hacking resources, we will pro up the noobs of the world and bring the community, at scale, to the next level of skill.

Come, listen, and learn how we can help!

1. link
2. Connor Nelson, Yan Shoshitaishvili. DOJO: Applied Cybersecurity Education In The Browser. ACM SIGCSE 2024. link
3. Connor Nelson, Yan Shoshitaishvili. PWN The Learning Curve: Education-First CTF Challenges. ACM SIGCSE 2024. link
4. link
5. link

Speakers: Yan "Zardus" Shoshitaishvili,Perri Adams

SpeakerBio: Yan "Zardus" Shoshitaishvili, Associate Professor at Arizona State University

Zardus (Yan Shoshitaishvili) is an Associate Professor at Arizona State University, where he pursues passions of cybersecurity research (focusing on binary analysis and exploitation) and education. Zardus has competed in CTFs for over 15 years, hosted DEF CON CTF, and led Shellphish's participation in the DARPA Cyber Grand Challengge.

In order to inspire students to pursue cybersecurity (and, ultimately, compete at DEF CON!), Yan created pwn.college, an open practice-makes-perfect learning platform that is revolutionizing cybersecurity education for aspiring hackers around the world.

SpeakerBio: Perri Adams, Special Assistant to the Director at Defense Advanced Research Projects Agency (DARPA)

Ms. Perri Adams is a special assistant to the director at DARPA, where she advises stakeholders at the agency and across the U.S. government on the next generation of AI and cybersecurity technology.

Prior to this role, Adams was a program manager within DARPA's Information Innovation Office (I2O), where, among other programs, she created the AI Cyber Challenge (AIxCC).

Adams has been an avid participant in cybersecurity CTF competitions and was one of the organizers of the DEF CON CTF. She holds a bachelor's degree in computer science from Rensselaer Polytechnic Institute and is a proud alumna of the computer security club, RPISEC.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 15:00-17:45 PDT

Title: DEF CON Closing Ceremonies & Awards
When: Sunday, Aug 11, 15:00 - 17:45 PDT
Where: LVCC West/Floor 1/Hall 1/Tracks 1-2 - Map

Description:
SpeakerBio: Jeff "The Dark Tangent" Moss, DEF CON Communications
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Friday - 18:00-18:20 PDT

Title: DEF CON Franklin Project
When: Friday, Aug 9, 18:00 - 18:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

DEF CON Franklin will infuse research from the hacker community into national security and foreign policy debates. We aim to lift up groundbreaking work happening across villages and deliver this critical research to key policymakers across the globe. Aside from policy work, Franklin will empower individual members of the community to volunteer directly with under-resourced critical infrastructure that support our world.

SpeakerBio: Jacob H Braun, Acting Principal Deputy National Cyber Director at Office of the National Cyber Director (ONCD)

Jake Braun served in the White House as Acting Principal Deputy National Cyber Director from May 2023 to July 2024. Prior to joining the White House Office of the National Cyber Director, he was appointed by President Joseph Biden as Senior Counselor to the Secretary of Homeland Security. Braun is also a lecturer at the University of Chicago's Harris School of Public Policy Studies and Chairman of the Cyber Policy Initiative there.

From 2009 to 2011, Braun served as White House Liaison to the U.S. Department of Homeland Security. Braun is also co-founder of the DEF CON Voting Machine Hacking Village (Voting Village) hacker conference."

Return to Index - Add to Google - ics Calendar file

DCG - Sunday - 10:00-12:59 PDT

Title: DEF CON Groups - Open for questions and hanging out
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 2/W236 - Map

Description:

Do you have questions about what DEF CON Groups are? Do you need help finding a group near you? Feel free to come ask. Or, just come up and hang out.

Return to Index - Add to Google - ics Calendar file

DCG - Saturday - 10:00-17:59 PDT

Title: DEF CON Groups - Open for questions and hanging out
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W236 - Map

Description:

Do you have questions about what DEF CON Groups are? Do you need help finding a group near you? Feel free to come ask. Or, just come up and hang out.

Return to Index - Add to Google - ics Calendar file

DCG - Friday - 10:00-17:59 PDT

Title: DEF CON Groups - Open for questions and hanging out
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W236 - Map

Description:

Do you have questions about what DEF CON Groups are? Do you need help finding a group near you? Feel free to come ask. Or, just come up and hang out.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 12:05-13:05 PDT

Title: DEF CON Groups Panel #1
When: Saturday, Aug 10, 12:05 - 13:05 PDT
Where: Virtual

Description:
Speakers: ET E,xray,TX,overcast,Abhishek S

SpeakerBio: ET E
No BIO available
SpeakerBio: xray
No BIO available
SpeakerBio: TX
No BIO available
SpeakerBio: overcast
No BIO available
SpeakerBio: Abhishek S, Security Engineer at Flipkart

Abhishek S is a Security Engineer at Flipkart with primary research focus in application security and red teaming. He is a staff of Adversary Village at (DEF CON) and an executive member of DC0471 group, he has been a speaker for various conferences like C0c0n 23 and Blackhat MEA 23. With over 4 years of experience playing CTF(s) and hunting for vulnerabilities in various VDP programs. He is listed in hall of fames of Google, Facebook, Microsoft and 40+ organizations for finding their security vulnerabilities. He has about four cve(s) from various organizations such as Android, Tenable, StrAPI CMS etc. currently holds various certifications such as OSCP, BSCP, CRTP, GIAC GFACT etc. Other than the technical side, he loves to travel around the world and is a automotive enthusiast.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 16:00-18:59 PDT

Title: DEF CON Holland Group Presents: VrijMiBo
When: Friday, Aug 9, 16:00 - 18:59 PDT
Where: LVCC West/Floor 2/HallwayCon Lounge past W234 - Map

Description:

In The Netherlands it's a tradition to catch up with your colleagues just before the end of the workday on Friday when the weekend starts to kick in. In The Netherlands this is called the "VrijMiBo" (Vrijdag/Friday - Middag/Afternoon Borrel/Drink)

"VrijMiBo/Friday afternoon Drink" at DEF CON is a perfect moment to talk about what your favorite thing is at DEF CON, show your cool handmade badges, impress other hackers about your latest hacks, make new friends, gossip about your boss and show your cat or dog pictures.

Vrijdag Middag Borrel, Freitag Mittags Getränk, Apéritif du vendredi après-midi, trago de viernes por la tarde.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 20:00-23:59 PDT

Title: DEF CON Movie Night
When: Saturday, Aug 10, 20:00 - 23:59 PDT
Where: LVCC West/Floor 3/W320 - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 20:00-23:59 PDT

Title: DEF CON Movie Night
When: Friday, Aug 9, 20:00 - 23:59 PDT
Where: LVCC West/Floor 3/W320 - Map

Description:

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: DEF CON Scavenger Hunt
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-02 - Map

Description:

Whether you're a seasoned DEFCON veteran or a curious newcomer, the DEFCON Scavenger Hunt promises to challenge your skills, tickle your wits, and ignite your hacker spirit. Our list is a portal to mystery, mischief, and mayhem. Assemble your team of up to five members, interpret the items, and submit your findings at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

Casual players will enjoy doing a handful of items, but you will need to devote your entire weekend if you want to win. It's not just about fame, glory, or boxes of swag; the true allure is the camaraderie of fellow hackers, the knowledge that you've etched your mark on DEFCON history, and the ultimate badge of honor: bragging rights. Nothing says "I'm a hacker" quite like being triumphant at the DEFCON Scavenger Hunt contest.

See you at the booth!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: DEF CON Scavenger Hunt
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-02 - Map

Description:

Whether you're a seasoned DEFCON veteran or a curious newcomer, the DEFCON Scavenger Hunt promises to challenge your skills, tickle your wits, and ignite your hacker spirit. Our list is a portal to mystery, mischief, and mayhem. Assemble your team of up to five members, interpret the items, and submit your findings at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

Casual players will enjoy doing a handful of items, but you will need to devote your entire weekend if you want to win. It's not just about fame, glory, or boxes of swag; the true allure is the camaraderie of fellow hackers, the knowledge that you've etched your mark on DEFCON history, and the ultimate badge of honor: bragging rights. Nothing says "I'm a hacker" quite like being triumphant at the DEFCON Scavenger Hunt contest.

See you at the booth!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: DEF CON Scavenger Hunt
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-02 - Map

Description:

Whether you're a seasoned DEFCON veteran or a curious newcomer, the DEFCON Scavenger Hunt promises to challenge your skills, tickle your wits, and ignite your hacker spirit. Our list is a portal to mystery, mischief, and mayhem. Assemble your team of up to five members, interpret the items, and submit your findings at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

Casual players will enjoy doing a handful of items, but you will need to devote your entire weekend if you want to win. It's not just about fame, glory, or boxes of swag; the true allure is the camaraderie of fellow hackers, the knowledge that you've etched your mark on DEFCON history, and the ultimate badge of honor: bragging rights. Nothing says "I'm a hacker" quite like being triumphant at the DEFCON Scavenger Hunt contest.

See you at the booth!

Return to Index - Add to Google - ics Calendar file

DC - Friday - 14:00-14:45 PDT

Title: DEF CON Unplugged: Cocktails & Cyber with Jeff & Jen
When: Friday, Aug 9, 14:00 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

Join DEF CON Founder Jeff Moss for an Ask Me Anything with CISA Director Jen Easterly. REAL WORLD DEF CON: Where hackers stop being polite and start getting real.

SpeakerBio: Jen Easterly, Director at Cybersecurity and Infrastructure Security Agency (CISA)

Jen Easterly is the Director of the Cybersecurity and Infrastructure Security Agency (CISA). She was nominated by President Biden in April 2021 and unanimously confirmed by the Senate on July 12, 2021. Before coming to CISA, Jen was Head of Firm Resilience at Morgan Stanley. A two-time recipient of the Bronze Star, Jen retired from the U.S. Army after more than 20 years, including deployments in Haiti, the Balkans, Iraq, and Afghanistan. Responsible for standing up the Army's first cyber battalion, she was also instrumental in the creation of United States Cyber Command. A graduate of West Point, Jen holds a master's degree from the University of Oxford, where she studied as a Rhodes Scholar. She is the recipient of numerous honors, including the George C. Marshall Award in Ethical Leadership and the National Defense University Admiral Grace Hopper Award. She is a proud Mom, a mental health advocate, a Rubik's Cube enthusiast, and an aspiring electric guitarist.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 05:00-07:59 PDT

Title: Defcon.run
When: Friday, Aug 9, 05:00 - 07:59 PDT
Where: Other / See Description

Description:

Thursday, Friday, Saturday and Sunday: 05:00 to 08:00, with random pop up meetings throughout the day in the con space.

Defcon.run is an evolution of the now long running DEF CON 4x5K running event. Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in small distributed groups around Las Vegas. It's the same old event but at a distributed scale!

Show up in the morning, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances. Full Information at https://defcon.run

Return to Index - Add to Google - ics Calendar file

MISC - Thursday - 05:00-07:59 PDT

Title: Defcon.run
When: Thursday, Aug 8, 05:00 - 07:59 PDT
Where: Other / See Description

Description:

Thursday, Friday, Saturday and Sunday: 05:00 to 08:00, with random pop up meetings throughout the day in the con space.

Defcon.run is an evolution of the now long running DEF CON 4x5K running event. Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in small distributed groups around Las Vegas. It's the same old event but at a distributed scale!

Show up in the morning, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances. Full Information at https://defcon.run

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 05:00-07:59 PDT

Title: Defcon.run
When: Saturday, Aug 10, 05:00 - 07:59 PDT
Where: Other / See Description

Description:

Thursday, Friday, Saturday and Sunday: 05:00 to 08:00, with random pop up meetings throughout the day in the con space.

Defcon.run is an evolution of the now long running DEF CON 4x5K running event. Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in small distributed groups around Las Vegas. It's the same old event but at a distributed scale!

Show up in the morning, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances. Full Information at https://defcon.run

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 05:00-07:59 PDT

Title: Defcon.run
When: Sunday, Aug 11, 05:00 - 07:59 PDT
Where: Other / See Description

Description:

Thursday, Friday, Saturday and Sunday: 05:00 to 08:00, with random pop up meetings throughout the day in the con space.

Defcon.run is an evolution of the now long running DEF CON 4x5K running event. Due to stupendous growth, we've been forced to change up the format. This year's activity will look to match up folks for fun runs, and rucks (!), in small distributed groups around Las Vegas. It's the same old event but at a distributed scale!

Show up in the morning, go for a run with folks, have a good time!

We'll have a full set of routes for people to choose from from simple 5Ks to more ambitious distances. Full Information at https://defcon.run

Return to Index - Add to Google - ics Calendar file

DC - Friday - 13:00-13:45 PDT

Title: Defeating EDR Evading Malware with Memory Forensics
When: Friday, Aug 9, 13:00 - 13:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Endpoint detection and response (EDR) software has gained significant market share due to its ability to examine system state for signs of malware and attacker activity well beyond what traditional anti-virus software is capable of detecting. This deep inspection capability of EDRs has led to an arms race with malware developers who want to evade EDRs while still achieving desired goals, such as code injection, lateral movement, and credential theft. This monitoring and evasion occurs in the lowest levels of hardware and software, including call stack frames, exception handlers, system calls, and manipulation of native instructions. Given this reality, EDRs are limited in how much lower they can operate to maintain an advantage. The success of EDR bypasses has led to their use in many high-profile attacks and by prolific ransomware groups.

In this talk, we discuss our research effort that led to the development of new memory forensics techniques for the detection of the bypasses that malware uses to evade EDRs. This includes bypass techniques, such as direct and indirect system calls, module overwriting, malicious exceptions handlers, and abuse of debug registers. Our developed capabilities were created as new plugins to the Volatility memory analysis framework, version 3, and will be released after the talk.

1. “Operation Dragon Castling: APT group targeting betting companies,” link, 2023.
2. “Defeating Guloader Anti-Analysis Technique,” link, 2023.
3. “A Deep Dive Into ALPHV/BlackCat Ransomware,” link, 2024.
4. “APT Operation Skeleton Key,” link, 2023.
5. “LockBit Ransomware Side-loads Cobalt Strike Beacon with Legitimate VMware Utility,” link, 2024.19
6. “BlueBravo Uses Ambassador Lure to Deploy,” link, 2024.
7. “UNMASKING THE DARK ART OF VECTORED EXCEPTION HANDLING: BYPASSING XDR AND EDR IN THE EVOLVING CYBER THREAT LANDSCAPE,” link, 2023.
8. “Dirty Vanity: A New Approach to Code injection & EDR by-pass,” link, 2022.
9. Volexity, “Surge Collect Pro,” link, 2022.
10. “capstone,” link, 2024.
11. “Silencing cylance: A case study in modern edrs,” link, 2019.
12. “Av/edr evasion — malware development p — 3,” link, 2023.
13. “A practical guide to bypassing userland api hooking,” link, 2022.
14. A. Case, A. Ali-Gombe, M. Sun, R. Maggio, M. Firoz-Ul-Amin, M. Jalalzai, and G. G. R. III, “HookTracer: A System for Automated and Accessible API Hooks Analysis,” Proceedings of the 18th Annual Digital Forensics Research Conference (DFRWS), 2019.
15. F. Block, “Windows memory forensics: Identification of (malicious) modifications in memory-mapped image files,” Forensic Science International: Digital Investigation, 2023. (Online). Available: link
16. F. Block and A. Dewald, “Windows memory forensics: Detecting (un)intentionally hidden injected code by examining page table entries,” Digital Investigation, vol. 29, pp. S3–S12, 07 2019.
17. “CCob,” link, 2024.
18. “Lets Create An EDR. . . And Bypass It! Part 1,” link, 2020.
19. “r77 rootkit,” link, 2024.
20. “Deep Vanity,” link, 2022. 20
21. “Peruns-Fart,” link, 2023.
22. “FREEZE – A PAYLOAD TOOLKIT FOR BYPASSING EDRS USING SUSPENDED PROCESSES,” link, 2023.
23. “Process Cloning,” link, 2023.
24. “APT Group Chimera,” link, 2022.
25. “Red Team Tactics: Combining Direct System Calls and sRDI to bypass AV/EDR,” link, 2019.
26. “Hell’s Gate,” link, 2020.
27. “Halo’s Gate,” link, 2021.
28. “Tartarus Gate,” link, 2021.

29. “Bypassing User-Mode Hooks and Direct Invocation of System Calls for Red Teams,” link, 2020.
30. “SysWhispers2,” link, 2022.
31. “An Introduction into Stack Spoofing,” link, 2023.
32. “SilentMoonwalk: Implementing a dynamic Call Stack Spoofer,” link, 2022.
33. “Spoofing Call Stacks To Confuse EDRs,” link, 2022.
34. “Behind the Mask: Spoofing Call Stacks Dynamically with Timers,” link, 2022.
35. “HellHall,” link, 2023.
36. link, 2008.
37. “Defeating Guloader Anti-Analysis Technique,” link, 2022.21
38. “GULoader Campaigns: A Deep Dive Analysis of a highly evasive Shellcode based loader,” link, 2023.
39. “Gh0stRat Anti-Debugging : Nested SEH (try - catch) to Decrypt and Load its Payload,” link, 2021.
40. “Syscalls via Vectored Exception Handling,” link, 2024.
41. “Bypassing AV/EDR Hooks via Vectored Syscall - POC,” link, 2022.
42. “MutationGate,” link, 2024.
43. Cymulate Research, “BlindSide,” link, 2023.
44. “In-Process Patchless AMSI Bypass,” link, 2022.
45. “PatchlessCLR,” link, 2022.
46. “Dumping the VEH in Windows 10,” link, 2020.
47. “Detecting anomalous Vectored Exception Handlers on Windows,” link, 2022.
48. “SetUnhandledExceptionFilter,” link, 2024.

Speakers: Andrew Case,Austin Sellers,Golden Richard,David McDonald,Gustavo Moreira

SpeakerBio: Andrew Case, Director of Research at Volexity

Andrew Case is the Director of Research at Volexity and has significant experience in incident response handling and malware analysis. He has conducted numerous large-scale investigations that span enterprises and industries. Case is a core developer of the Volatility memory analysis framework, and a co-author of the highly popular and technical forensics analysis book "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory."

SpeakerBio: Austin Sellers, Detection Engineer at Volexity

Austin Sellers is a Detection Engineer at Volexity where he focuses on automating large scale memory analysis and threat detection techniques. He has significant experience in developing memory analysis datasets that allow for automated verification and testing of kernel and userland memory forensics techniques.

SpeakerBio: Golden Richard, Professor of Computer Science and Engineering and Associate Director for Cybersecurity at Center for Computation and Technology (CCT) at LSU

Golden G. Richard III is a cybersecurity researcher and teacher and a Fellow of the American Academy of Forensic Sciences. He has over 40 years of practical experience in computer systems and computer security and is a devoted advocate for applied cybersecurity education. He is currently Professor of Computer Science and Engineering and Associate Director for Cybersecurity at the Center for Computation and Technology (CCT) at LSU. He also supports NSA's CAE-CO internship program, teaching memory forensics, vulnerability analysis, and other topics to cleared interns. His primary research interests are memory forensics, digital forensics, malware analysis, reverse engineering, and operating systems. Dr. Richard earned his BS in Computer Science from the University of New Orleans and MS and PhD in Computer Science from The Ohio State University.

SpeakerBio: David McDonald, Volcano team at Volexity

David McDonald is a researcher and software engineer with 3 years of digital forensics R&D experience. His passion for this field began with his involvement in the University of New Orleans CTF team, as well as through his time as a Systems Programming teaching assistant. After over two years of digital forensics research and development on Cellebrite's computer forensics team, he joined Volexity's Volcano team, where he now works to develop next-generation memory analysis

solutions.

SpeakerBio: Gustavo Moreira, Senior Security Engineer at Volexity

Gustavo Moreira is a Senior Security Engineer at Volexity. He has significant experience in reverse engineering, incident response handling, embedded systems development and security, Windows and Linux internals, and automation of large scale malware analysis.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 10:30-11:15 PDT

Title: Defeating magic by magic Using ALPC security features to compromise RPC services
When: Friday, Aug 9, 10:30 - 11:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Advanced Local Procedure Call (ALPC) is an Inter Process Communication method in the Windows kernel. In the past few years, Windows ALPC and RPC vulnerabilities have emerged in an endless stream. These vulnerabilities are mainly based on TOCTOU file operations, memory corruption vulnerabilities in RPC services and ALPC syscalls in ntoskrnl.

Windows kernel provides a variety of security measures to ensure that the data and context accepted by the ALPC and RPC servers are safe. We noticed the attack surface in the security mechanism of the ALPC kernel, and we found a security flaw in this mechanism (magic) and successfully obtained the system privilege from unauthorized users (defeating magic by magic).

In this talk, we will first overview the communication mechanism of ALPC and RPC services. We will discuss the details of ALPC and RPC in the marshal/unmarshal process that has not been disclosed before. We'll also talk about the kernel security mechanism in ALPC syscalls. Then we will analyze some historical bugs in ALPC and RPC, and disclose the details of the vulnerability we found, discussing how we bypassed the security mechanism through a small security flaw in security mechanisms. Later we'll discuss the exploitation, you will learn about the multiple ways. Finally, We'll make conclusions and share our opinions on this attack surface, including some tips and opinions on how to find these kinds of bugs.

1. A view into ALPC-RPC by Clement Rouault and Thomas Imbert Hack.lu 2017
2. Exploiting Errors in Windows Error Reporting - Gal De Leon
3. Windows Internals, Part 2, 7th Edition

Speakers: WangJunJie Zhang,YiSheng He

SpeakerBio: WangJunJie Zhang, Senior Security Researcher at Hillstone Network Security Research Institute

WangJunJie Zhang is a senior security researcher of Hillstone Network Security Research Institute. His work involved exploit development and bug hunting. He is currently focusing on windows components and kernel security and he has reported many vulnerabilities to Microsoft and RedHat and got acknowledgements. He was also listed on Microsoft Most Valuable Researcher from 2020 to 2023. He was also the speaker of CansecWest 2023 and HITBSecConf Amsterdam 2023 conference.

SpeakerBio: YiSheng He

YiSheng He is a member of OWASP, (ISC)², CSA and other organizations. He is the organizer of the DCG86020 event. He has obtained various international professional certifications such as CISSP, CCSK, CISA, and participated in many open source security projects. He obtained a large number of CVE numbers and received acknowledgements from Microsoft, Apple and other companies. He also participated in many CTF competitions and won good ranking. His research interests include AIoT and WEB security. He was also the speaker of CansecWest 2023 and HITBSecConf Amsterdam 2023 conference.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Defend the Airport CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

You are a new to the Airport IT staff at the IG International Airport Network Operations Center, working your first holiday travel weekend. It has been a busy day managing the network with the control tower reporting several small glitches.

No alerts have been raised in the network, and the glitches appeared to have been easily handled. While taking your last break of the day, you decide to take a short walk around the concourse to watch the sun set. Suddenly, your cell phone rings and the voice on the other end is a panicked Control Tower Operator. A short time earlier, the tower had observed the runway lights turn off, come back on, and are now randomly blinking. They also mentioned the Operator HMI (Human Machine Interface) controlling the Runway Lighting system is non-responsive and they are locked out of the Maintenance HMI to reboot the system. Time is critical – without the lights, the planes circling the airport cannot land. With limited fuel stores, the planes are unable to divert to another airport. You sit down at your terminal to pull up the maintenance manual and troubleshoot the problem only to discover you are locked out of your account. You are suddenly relieved that management would not let you deploy security updates to the network because they feared service interruptions may occur. Once you regain access to the system and have all the reference material available, you bring up the control logic for the runway lighting system on one screen and the HMIs on another and quickly realize this is not a normal system failure. An unknown hacker or hacker group has ceased and taken control of the system. They have manipulated the PLC's (Programmable Logic Controller) and impacted the HMIs. Time is of the essence to restore operation to the Runway Lighting control system before the planes run out of fuel.

SpeakerBio: IntelliGenesis and IG Labs
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Defend the Airport CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

You are a new to the Airport IT staff at the IG International Airport Network Operations Center, working your first holiday travel weekend. It has been a busy day managing the network with the control tower reporting several small glitches.

No alerts have been raised in the network, and the glitches appeared to have been easily handled. While taking your last break of the day, you decide to take a short walk around the concourse to watch the sun set. Suddenly, your cell phone rings and the voice on the other end is a panicked Control Tower Operator. A short time earlier, the tower had observed the runway lights turn off, come back on, and are now randomly blinking. They also mentioned the Operator HMI (Human Machine Interface) controlling the Runway Lighting system is non-responsive and they are locked out of the Maintenance HMI to reboot the system. Time is critical – without the lights, the planes circling the airport cannot land. With limited fuel stores, the planes are unable to divert to another airport. You sit down at your terminal to pull up the maintenance manual and troubleshoot the problem only to discover you are locked out of your account. You are suddenly relieved that management would not let you deploy security updates to the network because they feared service interruptions may occur. Once you regain access to the system and have all the reference material available, you bring up the control logic for the runway lighting system on one screen and the HMIs on another and quickly realize this is not a normal system failure. An unknown hacker or hacker group has ceased and taken control of the system. They have manipulated the PLC's (Programmable Logic Controller) and impacted the HMIs. Time is of the essence to restore operation to the Runway Lighting control system before the planes run out of fuel.

SpeakerBio: IntelliGenesis and IG Labs
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Defend the Airport CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

You are a new to the Airport IT staff at the IG International Airport Network Operations Center, working your first holiday travel weekend. It has been a busy day managing the network with the control tower reporting several small glitches.

No alerts have been raised in the network, and the glitches appeared to have been easily handled. While taking your last break of the day, you decide to take a short walk around the concourse to watch the sun set. Suddenly, your cell phone rings and the voice on the other end is a panicked Control Tower Operator. A short time earlier, the tower had observed the runway lights turn off, come back on, and are now randomly blinking. They also mentioned the Operator HMI (Human Machine Interface) controlling the Runway Lighting system is non-responsive and they are locked out of the Maintenance HMI to reboot the system. Time is critical – without the lights, the planes circling the airport cannot land. With limited fuel stores, the planes are unable to divert to another airport. You sit down at your terminal to pull up the maintenance manual and troubleshoot the problem only to discover you are locked out of your account. You are suddenly relieved that management would not let you deploy security updates to the network because they feared service interruptions may occur. Once you regain access to the system and have all the reference material available, you bring up the control logic for the runway lighting system on one screen and the HMIs on another and quickly realize this is not a normal system failure. An unknown hacker or hacker group has ceased and taken control of the system. They have manipulated the PLC's (Programmable Logic Controller) and impacted the HMIs. Time is of the essence to restore operation to the Runway Lighting control system before the planes run out of fuel.

SpeakerBio: IntelliGenesis and IG Labs
No BIO available

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 11:00-11:45 PDT

Title: Democracy From Around the World
When: Saturday, Aug 10, 11:00 - 11:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

America is the second largest democracy in the world. India is the largest. Indonesia is the third. Often times democracy is associated with American Values, but democracies around the globe all share a common thread and have an impact on each other. Join us to hear word=d

SpeakerBio: Harri Hursti
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 11:00-11:59 PDT

Title: Detección de Vulnerabilidades mediante Instrumentación y su Explotación
When: Sunday, Aug 11, 11:00 - 11:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

En esta presentación se explorará cómo nuestra estrategia de instrumentación basada en la librería Microsoft Detours permite una inspección de los procesos de software comercial presente en diferentes sistemas, enfocándose en operaciones privilegiadas del sistema de archivos. Se detallará cómo el uso de la instrumentación facilita la búsqueda sistemática y exhaustiva de vulnerabilidades en dichos procesos, identificando y explotando fallos de seguridad críticos presentes en algunos de ellos. El proyecto demuestra la efectividad de Detours para realizar análisis de seguridad avanzados y muestra cómo las vulnerabilidades encontradas pueden ser explotadas para evaluar su impacto en escenarios reales. Esta exposición enfatiza la importancia y la efectividad de la búsqueda de vulnerabilidades para fortalecer la seguridad en sistemas de IT y OT.

SpeakerBio: Asher Davila, IoT/OT Security Researcher at Palo Alto Networks

Asher Davila (@asher_davila) is an IoT/OT Security Researcher at Palo Alto Networks, leveraging his expertise in the intersection of software and hardware across IoT to IIoT, ICS, and critical infrastructure security. His work includes discovering and disclosing vulnerabilities and malware affecting these systems, alongside developing tools for reverse engineering and exploitation efforts. Asher has also presented his findings at multiple cybersecurity conferences and academic events.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Detect a Threat
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Can you spot suspicious items in packages? Try out your skills.

SpeakerBio: TSA

No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Detect a Threat
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Can you spot suspicious items in packages? Try out your skills.

SpeakerBio: TSA

No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Detect a Threat
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Can you spot suspicious items in packages? Try out your skills.

SpeakerBio: TSA

No BIO available

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 14:00-14:55 PDT

Title: Detouring Danger: Hunting Privileged File Operation Vulnerabilities in OT/ICS software
When: Friday, Aug 9, 14:00 - 14:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The Microsoft Detours library was leveraged to instrument the entire process environment of an engineering workstation in an operational technology/industrial control system (OT/ICS) setting. This approach allowed for the comprehensive monitoring and analysis of privileged file operations within these systems. Through this method, multiple vulnerabilities in SCADA software were identified and exploited, demonstrating the effective use of Detours for security research in critical infrastructure contexts. This presentation will discuss how the custom dynamic-link library (DLL) developed with Detours enabled the systematic examination of file operations, leading to the discovery of security flaws that were then exploited. The talk will showcase these exploitations, providing insight into the types of vulnerabilities that were uncovered and the potential implications for system security. The focus will be on demonstrating the importance of having an effective vulnerability hunting strategy in critical environments and showing real exploitation scenarios of the vulnerabilities found through this method.

SpeakerBio: Asher Davila, IoT/OT Security Researcher at Palo Alto Networks

Asher Davila (@asher_davila) is an IoT/OT Security Researcher at Palo Alto Networks, leveraging his expertise in the intersection of software and hardware across IoT to IIoT, ICS, and critical infrastructure security. His work includes discovering and disclosing vulnerabilities and malware affecting these systems, alongside developing tools for reverse engineering and exploitation efforts. Asher has also presented his findings at multiple cybersecurity conferences and academic events.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 12:00-12:50 PDT

Title: Developing Better Payloads with Automated Testing
When: Saturday, Aug 10, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Everyone else is doing automated testing - why aren't red teamers? Be confident your payload will execute, regardless of the options you picked, by integrating shellidate into your continuous integration pipelines!

SpeakerBio: Nick McClendon
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 11:00-11:50 PDT

Title: Developing Evilginx Phishlets
When: Saturday, Aug 10, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

While there are many phishlet templates available on the Internet, but it is rare that they work out-of-the-box for your specific scenario.

This workshop is designed for those who are new to the Evilginx tool, and may have not had hands-on experience developing custom phishlets on their local machine. This workshop aims to give attendees the tools needed to effectively configure phishlet 'yaml' files for their specific situation. Additionally, the workshop will survey the necessary components of the phishlet 'yaml' file, as well as covering useful features new to Evilginx3.

This workshop will not focus on the development of phishing emails, bypassing spam filters, or remotely deploying and protecting Evilginx infrastructure.

This workshop is meant for all levels of experience, but some familiarity with Evilginx prior to attendance will be extremely helpful.

SpeakerBio: Michael Donley
No BIO available

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 17:00-17:30 PDT

Title: DevSecOps of Quantum Computers
When: Friday, Aug 9, 17:00 - 17:30 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 10:00-10:59 PDT

Title: Differential privacy beyond algorithms: Challenges for successful deployment
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Differential privacy (DP) has been hailed as the gold standard of privacy-preserving data analysis, by providing strong privacy guarantees while still enabling use of potentially sensitive data. Formally, DP gives a mathematically rigorous worst-case bound on the maximum amount of information that can be learned about an individual's data from the output of a computation. In the past two decades, the privacy community has developed DP algorithms that satisfy this privacy guarantee and allow for accurate data analysis for a wide variety of computational problems and application domains. We have also begun to see a number of high-profile deployments of DP systems in practice, both at large technology companies and government entities. Despite the promise and success of DP thus far, there are a number of critical challenges left to be addressed before DP can be easily deployed in practice, including: mapping the mathematical privacy guarantees onto protection against real-world threats, developing explanations of its guarantees and tradeoffs for non-technical users, integration with other privacy & security tools, preventing misuse, and more.

SpeakerBio: Rachel Cummings, Associate Professor of Industrial Engineering and Operations Research at Columbia University

Dr. Rachel Cummings is an Associate Professor of Industrial Engineering and Operations Research and (by courtesy) Computer Science at Columbia University, where she is also a member of the Data Science Institute and co-chairs the Cybersecurity Research Center. She is also a Fellow at the Center for Democracy & Technology. Before joining Columbia, she was an Assistant Professor of Industrial and Systems Engineering and (by courtesy) Computer Science at the Georgia Institute of Technology, and she previously received her Ph.D. in Computing and Mathematical Sciences at the California Institute of Technology. Her research interests lie primarily in data privacy, with connections to machine learning, algorithmic economics, optimization, statistics, and public policy. Dr. Cummings is the recipient of numerous awards including an NSF CAREER award, a DARPA Young Faculty Award, a DARPA Director's Fellowship, an Early Career Impact Award, multiple industry research awards, a Provost's Teaching Award, two doctoral dissertation awards, and Best Paper Awards at DISC 2014, CCS 2021, and SaTML 2023. Dr. Cummings also serves on the ACM U.S. Technology Policy Committee, the IEEE Standards Association, and the Future of Privacy Forum's Advisory Board.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 13:30-14:15 PDT

Title: Digital Emblems: When markings are required under international law, but you don't have a rattle-can handy
When: Friday, Aug 9, 13:30 - 14:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

There are physical markings that are required under hundreds of different international laws, some governing transport of goods across national borders, some offering humanitarian protections on the battlefield, some seeking to protect the environment or genetic diversity… What they all have in common is that they're currently represented by visual marks applied to objects. Many of these processes are undergoing "digitalization," and becoming machine-readable, or electronically-signaled. A standards effort currently underway in the IETF seeks to create a common global marking protocol which would allow open-standards-based devices to scan, cryptographically validate, and display the digital versions of these marks. This session will relate the state of the standards effort, the scope of markings that have been considered thus far, and seek input on security or privacy vulnerabilities which may exist in the proposed standard.

SpeakerBio: Bill Woodcock, Executive Director at Packet Clearing House

Bill Woodcock is the executive director of Packet Clearing House, the intergovernmental treaty organization that supports the operation of critical Internet infrastructure, including Internet exchange points and the core of the domain name system. Since entering the Internet industry in 1985, Bill has helped establish more than three hundred Internet exchange points. In 1989, Bill developed the anycast routing technique that now protects the domain name system. In 1998 he was one of the principal drivers of California 17538.4, the world's first anti-spam legislation. Bill was principal author of the Multicast DNS and Operator Requirements of Infrastructure Management Methods IETF drafts. In 2002 he co-founded INOC-DBA, the security-coordination hotline system that interconnects the network operations centers of more than three thousand Internet Service Providers and Security Operations Centers around the world. And in 2007, Bill was one of the two international liaisons deployed by NSP-Sec to the Estonian CERT during the Russian cyber-attack. In 2011, Bill authored the first survey of Internet interconnection agreements, as input to the OECD's analysis of the Internet economy. Bill served on the Global Commission on the Stability of Cyberspace and on the Commission on Caribbean Communications Resilience. He's on the board of directors of the M3AA Foundation, and was on the board of the American Registry for Internet Numbers for fifteen years. Now, Bill's work focuses principally on the security and economic stability of critical Internet infrastructure.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 14:00-14:45 PDT

Title: Discovering and exploiting local attacks against the 1Password MacOS desktop application
When: Saturday, Aug 10, 14:00 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Password managers are routinely granted a massive level of trust from users, by nature of managing some of their most sensitive credentials. For any noteworthy password manager, the encryption standards for user data are well understood and highly scrutinized. What is less understood is the attack surface of the software itself. This presentation explores the local security of the 1Password MacOS desktop application and answers the question of "how safe are my passwords if my computer is infected or otherwise compromised?".

This talk will cover the outcome of our research into 1Password, presenting several different attacks to dump local 1Password vaults. This includes describing multiple application vulnerabilities and security weaknesses we identified in the 1Password MacOS desktop application, as well as discussing the inherent limitations in its usage of IPC mechanisms and open source software. Additionally, we will discuss novel vulnerabilities found in Google Chrome that aided our exploitation of the 1Password browser extension.

DarthNull's work around decrypting 1Password vaults: link

Speakers:Jeffrey Hofmann,Colby Morgan

SpeakerBio: Jeffrey Hofmann, Senior Offensive Security Engineer

Jeffrey Hofmann is a Senior Offensive Security Engineer with a history of vulnerability research and exploit development. He recreated NSO's 0 click iOS exploit FORCEDENTRY and discovered pre-auth RCEs in the MDM KACE SMA.

SpeakerBio: Colby Morgan, Leads, Pentest Team at Robinhood

Colby Morgan is a Staff Offensive Security Engineer with extensive application and infrastructure security experience. Colby currently leads the pentest team at Robinhood.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 12:00-12:45 PDT

Title: Disenshittify or die! How hackers can seize the means of computation and build a new, good internet that is hardened against our asshole bosses' insatiable horniness for enshittification.

When: Saturday, Aug 10, 12:00 - 12:45 PDT

Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

The enshittification of the internet wasn't inevitable. The old, good internet gave way to the enshitternet because we let our bosses enshittify it. We took away the constraints of competition, regulation, interop and tech worker power, and so when our bosses yanked on the big enshittification lever in the c-suite, it started to budge further and further, toward total enshittification. A new, good internet is possible - and necessary - and it needs *you*.

SpeakerBio: Cory Doctorow, Author

Cory Doctorow is a science fiction author, activist and journalist. He is the author of many books, most recently THE BEZZLE and THE LOST CAUSE. In 2020, he was inducted into the Canadian Science Fiction and Fantasy Hall of Fame.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 12:00-13:45 PDT

Title: distribRuted - Distributed Attack Framework
When: Friday, Aug 9, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W303 - Map

Description:

Penetration testing tools often face limitations such as IP blocking, insufficient computing power, and time constraints. However, by executing these tests across a distributed network of hundreds of devices, these challenges can be overcome. Organizing such a large-scale attack efficiently is complex, as the number of nodes increases, so does the difficulty in orchestration and management. distribRuted provides the necessary infrastructure and orchestration for distributed attacks. This framework allows developers to easily create and execute specific distributed attacks using standard application modules. Users can develop their attack modules or utilize pre-existing ones from the community. With distribRuted, automating, managing, and tracking a distributed attack across hundreds of nodes becomes straightforward, thereby enhancing efficiency, reducing time and costs, and eliminating Single Point of Failure (SPoF) in penetration testing.

Speakers: Ismail Melih Tas,Numan Ozdemir

SpeakerBio: Ismail Melih Tas, Founder and CEO at Siber Ninja

Melih Tas is a VP in Application Security at a multi-national financial company in London, UK, and the founder and CEO of VulnHero and Siber Ninja, two cybersecurity startups. He has previously worked as a Senior Security Consultant at Synopsys, a Tech Lead at Garanti BBVA Bank, and a Security Researcher at Nortel-Networks Netas. Melih holds a Ph.D. in Cyber Security, has presented at renowned hacker conferences including DEF CON and Black Hat, and is a published academic author with a focus on VoIP security and Application Security.

SpeakerBio: Numan Ozdemir, Cybersecurity Researcher and Computer Programmer

Numan Ozdemir is a cybersecurity researcher and computer programmer currently pursuing a degree in Mathematics and Computer Science. His research interests include blockchain and application security.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 10:00-11:45 PDT

Title: Docker Exploitation Framework
When: Friday, Aug 9, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W303 - Map

Description:

Docker Exploitation Framework is a cross-platform framework that is focused on attacking container environments (think Kubernetes, docker, etc). It can identify vulnerabilities, misconfigurations, and potential attack vectors. It also helps to automate different stages of a successful kill-chain through features such as:

- Vulnerability scanning
- Container breakouts
- Pod2pod lateral movement
- File layers deep inspection and extraction
- Attack surface discovery and mapping
- Privilege escalation, etc

Speakers: Emmanuel Law,Rohit Pitke

SpeakerBio: Emmanuel Law, Senior Staff Security Engineer

Emmanuel Law (@libnex) has over a decade of security research experience. He has presented at various international conferences such as Black Hat USA Arsenal, Troopers, Kiwicon, Ruxcon etc. He has also released tools such as Shadow Workers for browser exploitation. He is currently working as a Senior Staff Security Engineer in San Francisco Bay Area.

SpeakerBio: Rohit Pitke

Rohit Pitke has been working in the security industry over a decade in various fields like application and infrastructure security, offensive security and security software development. He has presented in various conferences like AppSec USA, AppSec Rome, NullCon.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 10:00-10:30 PDT

Title: Does the World Need Another Threat Model, the Road to EMB3D
When: Friday, Aug 9, 10:00 - 10:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

With all the various threat model frameworks available, STRIDE, Trike, PASTA, VAST, etc., does the world need another one?

That was the question that shaped the creation of EMB3D, a threat model framework built around embedded systems (specifically in critical infrastructure) that addresses all phases of a threat to them: from the theorical/academic, proof of concept and exploit, to observed adversarial behavior.

But the goal was greater than just the threat framework, it was to bring a common language to the global community to discuss weaknesses and threats while striving to bring transparency to what are considered “black box” electronic systems.

In this presentation, we take you on the journey of how we went from venting about needing more transparency and accountability in the OT/ICS space to developing a new global threat model for embedded systems.

Speakers: Niyo Little Thunder Pearson,Jack Cyprus,Wyatt Ford

SpeakerBio: Niyo Little Thunder Pearson
No BIO available
SpeakerBio: Jack Cyprus
No BIO available
SpeakerBio: Wyatt Ford, Senior Software Engineer and Engineering Manager at Red Balloon Security

Wyatt Ford (@whyitfor) is a senior software engineer and engineering manager at Red Balloon Security and a core maintainer of OFRAK.

Return to Index - Add to Google - ics Calendar file

Title: DoH Deception: Evading ML-Based Tunnel Detection with Black-Box Attack Techniques
When: Saturday, Aug 10, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

This presentation is part of a graduate research project that delves into the vulnerabilities of Machine Learning (ML) models specifically designed to detect DNS Over HTTPS (DoH) tunnels. Previous research has primarily focused on developing models that prioritize accuracy and explainability. However, these studies have often overlooked the potential of adversarial attacks, leaving the models vulnerable to common adversarial attacks like black-box attacks. This presentation will demonstrate that all cutting-edge DoH tunnel detection models are vulnerable to black-box attacks. Our approach leverages real-world input data generated by DoH tunnel tools, which are constrained in the attack algorithm.

Moreover, we will show specific vulnerable features that model developers should avoid. When this feature type is considered, we successfully evaded all DoH tunnel detection models without using advanced techniques.

Notably, the audience can use the same methods to evade most Machine Learning-Based Network Intrusion Detection Systems, underlining our findings' immediate and practical implications.

ght Scholarship at the University of Arizona and the University of Florida, focusing on malware analysis. Additionally, Emanuel actively contributes to the OWASP Top 10 for LLM Apps. Committed to advancing cybersecurity technology, he shares his expertise through speaking engagements and research collaborations.

This presentation will dive into attacking ML DoH tunnel detection models using adversarial attack techniques for evasion. The key discussion points are as follows:

1 DNS tunnels In this section, we will discuss the evolution of DNS. We will explain why DNS over HTTPS (DoH) was conceived, what motivations drove it, and why vulnerabilities from its predecessor tried to mitigate them. Next, we will demonstrate how attackers can leverage DNS and DoH to create tunnels, which are covert channels for communication that bypass traditional network security measures. These tunnels can be used to exfiltrate information or as C&C (Command and Control) communication channels for malicious activities. Additionally, we will highlight the most popular tools for creating these tunnels using DoH.

2 DoH Tunnel Detection Models This section will discuss the primary datasets the scientific community uses to create ML models for detecting DoH tunnels. We will highlight how to extract features from DoH requests and which are the most used. We will also address the gaps and bad practices in these datasets that lead to developing vulnerable models. Additionally, we will show the best practices for building DoH tunnel detection models, such as choosing the best algorithms, implementing robust feature engineering techniques, and selecting the most relevant features for the model.

3 Adversarial Attacks This section will introduce adversarial attacks, a type of attack that aims to deceive or mislead a machine learning model by providing it with maliciously crafted input data. We will explain how 'white' and 'black' attacks on ML models are executed and how they differ. Furthermore, we will explain how to adapt 'black-box attacks, a type of adversarial attack where the attacker does not know the internal workings of the model, to target DoH tunnel detection models and similar models.

4 Attacking (DEMOs) This section will present demos covering the following scenarios: First, we will demonstrate how basic black-box attacks work for attacking DoH tunnel detection models. Next, we will show a demo using previous attacks, but this time, we will incorporate real-world inputs from DoH tunnel detection tools, constraining the attack algorithm. We will also identify vulnerable features within the dataset that attackers can exploit to bypass the DoH tunnel detection models. Additionally, we will release a patched open-source tool, dnstt, to consider all considered scenarios. Note: The demonstrations will be conducted live, but we will have pre-recorded videos to ensure continuity in case of any issues.

5 Defending This section will explain how to defend against the attacks presented earlier and demonstrate 'good practices and techniques' for protecting against them. We will also show how to build a robust model trained with adversarial attack samples generated from previous attacks, which can help improve the model's resilience to future attacks.

6 Next Steps In the final section, we will outline the future steps in our research and discuss the remaining gaps. We warmly invite new contributors to join our research efforts, as your insights and expertise can significantly advance our understanding in this field. Links:

Experiments (Attacking DoH tunnel detection models): link

Black Box Attack: Zero Order Optimization Attack, constrained to support real doh tunnel tools inputs: link

Dnstt patch (ongoing): You can now run it separately (dnstt + patch). The provided code does exactly that: link

SpeakerBio: Emanuel Valente
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Don't Give Up The Ship! Maritime SOC/NOC Afloat
When: Saturday, Aug 10, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

Defending a vessel's IT and OT systems while underway can be a matter of life and death. Cliff, Brad, and Phil present a framework for developing 24/7 network and security operations for vessels, addressing such technical topics as limited bandwidth/latency, detection and response, pre-planned actions, and an underway readiness dashboard. We will address technical and risk-management strategies for a SOC and NOC, including how we use a lab environment to simulate security operations for vessels underway.

Speakers: Philip Acosta,Cliff Neve,Brad Proctor

SpeakerBio: Philip Acosta, Founder and CEO at GuROO LLC

Phillip Acosta is the founder and CEO of GuROO LLC. With over 20 years of experience across the federal government in enterprise IT services, secure unified communications, and network engineering, Phil has led the charge to bring Network Operations-as-a-Service (NOCaaS) and cutting-edge communications services to the maritime industry. GuROO is currently delivering NOCaaS to the National Security Maritime Vessel (NSMV) fleet, a new class of vessel primarily utilized as a training vessel for the maritime academies. GuROO is also engaged with several maritime-focused autonomous unmanned platform providers to connect multiple UxVs for oceanographic research, monitoring, and freedom of navigation.

SpeakerBio: Cliff Neve, Vice President of Maritime Cybersecurity at MAD Security

Cliff Neve is the Vice President of Maritime Cybersecurity at MAD Security. He is a 1993 US Coast Guard Academy graduate and a retired Coast Guard Commander with 30 years of IT and cybersecurity leadership in the military and industry. He has served as the acting Deputy of Coast Guard Cyber Command and was instrumental in establishing CGCYBER and MAD's Maritime Security Operations Center, and also served as Deputy CIO of the White House Communications Agency. Cliff has consulted for maritime ports, shipping companies, the US Coast Guard, and the Department of Transportation's Maritime Administration (MARAD). His deep commitment to securing the Maritime Transportation System drives his advocacy efforts to find innovative and effective ways of securing information and systems in the maritime environment.

SpeakerBio: Brad Proctor
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 13:00-13:45 PDT

Title: Don't go too far… your job is not done!
When: Saturday, Aug 10, 13:00 - 13:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:
SpeakerBio: Chris Cleary
No BIO available

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 13:00-13:25 PDT

Title: Don't Ship Your Bridges! Tools to Explore Wireless Attack Surfaces in Every Ship's Marine Navigation Systems
When: Saturday, Aug 10, 13:00 - 13:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

In collaboration with the legendary Kess, the presenters will demonstrate a FOSS (gnuradio) based SDR tool for accessing and exploring wireless attack surfaces present on every ship and large maritime vessel. We will demonstrate abuse of the AIS protocol to cause various forms of mischief, including causing marine navigation and telemetry systems to hallucinate other major vessels and obstructions.

Speakers: Nick Halt,Duncan Woodbury

SpeakerBio: Nick Halt
No BIO available
SpeakerBio: Duncan Woodbury
No BIO available

Return to Index - Add to Google - ics Calendar file

LPV - Friday - 13:30-13:59 PDT

Title: Doors, Cameras, & Mantraps: Oh my!
When: Friday, Aug 9, 13:30 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

This is an entry level talk about the practical parts of Physical Security Assessment, and how to talk to clients.

SpeakerBio: Dylan "The Magician" Baklor, Web Application Pentester and Network Security Pentester at Macy's

Dylan Baklor, known by the handle "The Magician," is a seasoned security professional with extensive experience in both physical and network security. With 1.5 years dedicated to Physical Penetration Testing at Goldsky Security, Dylan developed and implemented comprehensive Physical Security testing Policies and Procedures, conducted rigorous testing, and provided actionable remediation recommendations. Notable, albeit unconventional, achievements include discovering network racks in restrooms and breaching a satellite manufacturing facility with compressed air. Holding certifications such as Pentest+, Security+, Network+, and CISSP, Dylan is continuously expanding their expertise. Currently, Dylan works at Macy's as a Web Application Pentester and Network Security Pentester, with a particular passion for wireless technologies including RFID, Bluetooth, and WiFi. Known for teaching clients how to identify and rectify their own security vulnerabilities, Dylan emphasizes practical knowledge and hands-on interaction. An engaging speaker on the fundamentals of physical security, Dylan is also a Cyborg, please ask him about it!

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 12:30-12:55 PDT

Title: DoorSim - making my conference travel easier
When: Saturday, Aug 10, 12:30 - 12:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

Earlier this year, I traveled with 2 full suitcases and shipped a 30lbs box to a conference, just to bring along a few readers, a few EACS and mini-doors for a small RFID village. I wanted to make that easier, so this talk will run through the process of planning, designing, and building a better solution, and hopefully make it easier for others to do the same.

SpeakerBio: evildaemond (Adam Foster)

evildaemond is a person who works in information security, with focuses in hardware, web pentesting and physsec, and regularly teaches lockpicking and physsec at conferences across Australia. They've released projects like the physsec-methodlogy, enjoys bug bounty and vulnerability disclosure, and has spent more money on stickers than some companies.

Return to Index - Add to Google - ics Calendar file

LPV - Saturday - 12:00-14:59 PDT

Title: Dozier Drill Tournament
When: Saturday, Aug 10, 12:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03-A - Map

Description:

Have you ever wanted to break out of handcuffs, pick open a closed bag and shoot your buddy in the chest with a nerf gun? So have we, that's why TOOOL presents the Dozer Drill. A fast paced skill based game where you have to free yourself from handcuffs, open a closed bag, and retrieve the nerf gun to be the first to hit the target. Join us on Friday for qualifiers, through the con for unofficial games, and on Saturday for an official bracket tournament.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 11:00-11:45 PDT

Title: Dragon SlayingGuide: Bug Hunting In VMware Device Virtualization
When: Sunday, Aug 11, 11:00 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

In this presentation, we will unveil a new attack surface: Device Virtualization in VMKernel. This isan unknown territory that has not been explored by security researchers to date. During the reverse engineering of the VMware Hypervisor, we discovered 8 vulnerabilities related to device virtualization, 3 of them have been assigned CVE number (some vulnerabilities have even been successfully exploited in Tianfu Cup), and the remaining 5 of our vulnerabilities have been officially confirmed by VMware.

Firstly we will delve into the loading process of vmm, the implementation of data sharing between vmm and vmx, and VMware's UserRPC, which facilitates communication between the Hypervisor and the Host. These mechanisms are crucial in virtual device emulation.

Then We will explain security issues in various parts of the USB system, including the host controller, VUsb middleware, and VUsb backend devices, based on the vulnerabilities we have unearthed.

In the end, We will primarily discuss the similarities and differences in SCSI-related device emulation in the virtual disk system between VMware Workstation and ESXi Additionally, we will cover design flaws related to disk device emulation that we discovered in VMKernel.

1. link
2. link
3. link
4. link
5. link
6. link
7. link
8. link
9. link
10. link
11. link
12. link
13. link
14. link
15. link
16. link
17. link conferences, including Usenix 2021, ACM CCS 2022, EuroS&P 2022, HITBSecConf2022, BlackHat Asia 2024.

Speakers: JiaQing Huang,Hao Zheng,Yue Liu

SpeakerBio: JiaQing Huang, Security Researcher, TianGong Team of Legendsec at QI-ANXIN Group

JiaQing Huang is a security researcher at TianGong Team of Legendsec at QI-ANXIN Group. He is currently focused on IoT and Virtualization security, having submitted multiple security vulnerabilities to VMware. In 2023, he and his teammate successfully escaped the Parallels Desktop at GeekCon2023.

SpeakerBio: Hao Zheng, Security Researcher, TianGong Team of Legendsec at QI-ANXIN Group

Hao Zheng is a security researcher at TianGong Team of Legendsec at QI-ANXIN Group. His focus is on Virtualization Security, having submitted multiple security vulnerabilities to VMware. In 2023, he and his teammate successfully escaped the Parallels Desktop at GeekCon2023.

SpeakerBio: Yue Liu, Security Researcher at QI-ANXIN Group

Yue Liu is a Security Researcher at QI-ANXIN Group, and the team leader of QI-ANXIN TianGong Team. He and his team has found lots of bugs in Windows/Android/ChromeOS/IoT Devices and cracked multiple targets in Tianfu Cup 2019/2020, GeekPwn 2020/2021/2022, GeekCon 2023. He has published his work in various conferences, including Usenix 2021, ACM CCS 2022, EuroS&P 2022, HITBSecConf2022, BlackHat Asia 2024.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 12:00-12:45 PDT

Title: DriverJack: Turning NTFS and Emulated Read-only Filesystems in an Infection and Persistence Vector
When: Sunday, Aug 11, 12:00 - 12:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

This article reassesses complex cyberattack tactics, focusing specifically on existing security measures and emerging weaknesses. We begin our investigation by examining initial methods of deployment in contemporary attacks, including those that focus on simulated read-only filesystems and NTFS vulnerabilities. Since the improvements made to the Windows security architecture in 2011, which include the enforcement of Driver Signature Enforcement (DSE) and Hypervisor-protected Code Integrity (HVCI), the nature of cyber threats has changed, requiring new ways to carry out attacks.

Our research presents a new method that takes advantage of previously uncovered weaknesses in emulated filesystems, allowing attackers to covertly install and maintain harmful programs. In addition, we uncover new NTFS vulnerabilities that enable attackers to conceal their presence and sustain persistence within victim systems. The study also investigates alternate methods for delivering and executing malware in usermode. In addition, we discuss several Indicators of Compromise (IOCs) to identify and detect these tactics.

1. link
2. link
3. link
4. link
5. link
6. link

SpeakerBio: Alessandro Magnosi, Managing Consultant and R&D Lead at BSI

I am a Managing Consultant with more than 10 years of experience in the IT field. Currently, I am part of the Security Testing Team at BSI, which is the UK national standards body, and a Global certification, training and cybersecurity firm. On top of my normal work, I work as an independent researcher for Synack RT and Cobalt, and an independent OSS developer in my spare time.

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Drone Capture the Flag (CTF)
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Put your drone hacking skills to the test in our Drone CTF. This advanced challenge requires participants to take over a drone mid-flight and develop a payload to hack a DJI drone. This CTF is perfect for those who have some experience in drone hacking or have participated in our Drone Hacking Workshop. It's a great opportunity to showcase your technical prowess and win some cool prizes.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Drone Capture the Flag (CTF)
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Put your drone hacking skills to the test in our Drone CTF. This advanced challenge requires participants to take over a drone mid-flight and develop a payload to hack a DJI drone. This CTF is perfect for those who have some experience in drone hacking or have participated in our Drone Hacking Workshop. It's a great opportunity to showcase your technical prowess and win some cool prizes.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Drone Capture the Flag (CTF)
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Put your drone hacking skills to the test in our Drone CTF. This advanced challenge requires participants to take over a drone mid-flight and develop a payload to hack a DJI drone. This CTF is perfect for those who have some experience in drone hacking or have participated in our Drone Hacking Workshop. It's a great opportunity to showcase your technical prowess and win some cool prizes.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Drone Flying Experience
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Experience the thrill of flying a drone in our custom-built cage right on the showroom floor. This activity is designed for everyone to enjoy, from kids to adults. Fly mini drones around the cage and see how well you can control these agile little machines. It's a fun, interactive way to learn the basics of drone piloting in a safe environment.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Drone Flying Experience
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Experience the thrill of flying a drone in our custom-built cage right on the showroom floor. This activity is designed for everyone to enjoy, from kids to adults. Fly mini drones around the cage and see how well you can control these agile little machines. It's a fun, interactive way to learn the basics of drone piloting in a safe environment.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Drone Flying Experience
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Experience the thrill of flying a drone in our custom-built cage right on the showroom floor. This activity is designed for everyone to enjoy, from kids to adults. Fly mini drones around the cage and see how well you can control these agile little machines. It's a fun, interactive way to learn the basics of drone piloting in a safe environment.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Drone Hacking Activity
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Join our Drone Hacking Activity and get hands-on experience with hacking into drone microcontrollers. This three-step in-depth activity is designed to teach you about the vulnerabilities and security of autonomous systems. Using sample drones, participants will learn techniques used in government pen tests. This workshop is suitable for all skill levels, from beginners to advanced hackers. Come and test your skills in a real-world scenario and understand the intricacies of drone security.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Drone Hacking Activity
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Join our Drone Hacking Activity and get hands-on experience with hacking into drone microcontrollers. This three-step in-depth activity is designed to teach you about the vulnerabilities and security of autonomous systems. Using sample drones, participants will learn techniques used in government pen tests. This workshop is suitable for all skill levels, from beginners to advanced hackers. Come and test your skills in a real-world scenario and understand the intricacies of drone security.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Drone Hacking Activity
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Join our Drone Hacking Activity and get hands-on experience with hacking into drone microcontrollers. This three-step in-depth activity is designed to teach you about the vulnerabilities and security of autonomous systems. Using sample drones, participants will learn techniques used in government pen tests. This workshop is suitable for all skill levels, from beginners to advanced hackers. Come and test your skills in a real-world scenario and understand the intricacies of drone security.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Drone Hacking Choose Your Own Adventure
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Dive into our interactive choose-your-own-adventure web interface and learn how to hack a drone in a fun, storyboard-based game. This graphical user interface simulates the process we use when hacking drones for the Air Force, allowing participants to make decisions and see the outcomes. It's a beginner-friendly activity that anyone can enjoy, offering insight into the steps involved in drone penetration testing.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Drone Hacking Choose Your Own Adventure
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Dive into our interactive choose-your-own-adventure web interface and learn how to hack a drone in a fun, storyboard-based game. This graphical user interface simulates the process we use when hacking drones for the Air Force, allowing participants to make decisions and see the outcomes. It's a beginner-friendly activity that anyone can enjoy, offering insight into the steps involved in drone penetration testing.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Drone Hacking Choose Your Own Adventure
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Dive into our interactive choose-your-own-adventure web interface and learn how to hack a drone in a fun, storyboard-based game. This graphical user interface simulates the process we use when hacking drones for the Air Force, allowing participants to make decisions and see the outcomes. It's a beginner-friendly activity that anyone can enjoy, offering insight into the steps involved in drone penetration testing.

SpeakerBio: Dark Wolf
No BIO available

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 14:00-15:45 PDT

Title: Drop-Pi
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W306 - Map

Description:

The Drop-Pi is a suite of software developed on a Raspberry Pi to facilitate the automatic bypassing of 802.1x/NAC implementations (pre 802.1x-2010 standards) and establish discrete remote access into target networks. Designed with physical penetration testing in mind, the Drop-Pi can establish remote access inside a target network within a matter of seconds after being plugged in, affording assessors with a quick in and out on an objective. Its built with common and easily sourced hardware which allows for easy and quick provisioning of multiple Drop-Pi devices. When it's not feasible to utilize a target network for egress traffic, the Drop-Pi can easily be configured to employ a wireless connection or mobile hotspot to facilitate access in and out of the network.

Speakers: Doug Kent,Robert Ditmer

SpeakerBio: Doug Kent, Pentesting Team at State Farm

Doug has worked at State Farm for about 20 years. Working on mostly security technologies ranging from Active Directory, PKI, Endpoint protection and finally landing recently on the Pentesting team. Doug has a passion for identifying vulnerabilities and partnering with control solution teams to protect State Farm data and fulfill our promise to customers. He strives to help others with offensive security skills by providing training, guidance, and kill chain demonstrations.

SpeakerBio: Robert Ditmer, Red Team at State Farm

Rob has been on the State Farm Pentesting Team for 3 years and has recently moved the Red Team. Prior to his time at State Farm, he has worked with various other companies as a penetration testing consultant - enabling him to experience a wide range of technologies and their differing implementations. Rob enjoys the challenge of developing tools and infrastructure to better the skills and abilities of the State Farms Red Team.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Dumb Terminal fun
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

We will have several dumb terminals available for all sorts of things courtesy of SCAVHUNT!

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-15:59 PDT

Title: Dumb Terminal fun
When: Saturday, Aug 10, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

We will have several dumb terminals available for all sorts of things courtesy of SCAVHUNT!

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-15:59 PDT

Title: Dumb Terminal fun
When: Friday, Aug 9, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

We will have several dumb terminals available for all sorts of things courtesy of SCAVHUNT!

Return to Index - Add to Google - ics Calendar file

BHV - Friday - 15:30-15:59 PDT

Title: Dysfunctional Unity: The Road to Nowhere
When: Friday, Aug 9, 15:30 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Years progress, time passes, and medical devices are still vulnerable, with Hospital computer and network security being a hot topic on the minds of citizens and CISA/FDA/etc. If we do not get better now, things will get much worse in the future. My talk will cover some general mistakes observed within the Medical device topography, misnomers about SBOM and what it is and what it accomplishes, ideas for roadmaps for more secure devices and environments and discussions around CVEs relating to the medical device topography.

SpeakerBio: Michael "v3ga" Aguilar, Principle Consultant at Secureworks Adversary Group

Michael Aguilar (v3ga) is a Principle Consultant for Secureworks Adversary Group. He runs Adversary Simulation operations, Physical Security and Network/Web based assessments as well as Adversarial Medical Device Tests. When not doing computer things, he reads a lot and likes to run to de-stress. He is also an avid fan of playing guitar really fast and screaming at people.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 18:30-21:30 PDT

Title: EFF Tech Trivia
When: Saturday, Aug 10, 18:30 - 21:30 PDT
Where: LVCC West/Floor 3/W307-W308 - Map

Description:

EFF's team of technology experts have crafted challenging trivia about the fascinating, obscure, and trivial aspects of digital security, online rights, and Internet culture. Competing teams will plumb the unfathomable depths of their knowledge, but only the champion hive mind will claim the First Place Tech Trivia Trophy and EFF swag pack. The second and third place teams will also win great EFF gear.

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 14:00-14:30 PDT

Title: Efficient Bug Bounty Automation Techniques
When: Saturday, Aug 10, 14:00 - 14:30 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

If you're a bug bounty hunter, time can literally mean money. For this reason, automation can be a vital part of how you hunt. But automation has limits. Whether this is hardware limits, target rate limits, WAFs & bot detection, and the list goes on. Successful automation techniques should EFFICIENTLY enhance your hunting. Whether it is being first to a fresh target, or finding targets other hunters haven't. We will go over some techniques and tools to get ahead of the pack, without wasting all your time and money.

SpeakerBio: Gunnar Andrews

I am a hacker, engineer, gamer, and creator from the Midwest. I enjoy being involved in the bug bounty community, meeting new hunters, learning techniques, and building cool software! I have a passion for writing security tools and building systems, as well as creating the best and biggest community of friends I can! I love to talk automation, hacking, software/systems, and just about anything else tech.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-11:59 PDT

Title: Egor's Keyboard Corner
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Keyboard Corner hosts typing challenges that test the speed and accuracy of attendees' typing skills on various keyboards. Participants can compete for high scores and bragging rights in a friendly and competitive setting. This activity adds an element of fun and excitement to the conference while highlighting the importance of efficient typing in cybersecurity.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Egor's Keyboard Corner
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Keyboard Corner hosts typing challenges that test the speed and accuracy of attendees' typing skills on various keyboards. Participants can compete for high scores and bragging rights in a friendly and competitive setting. This activity adds an element of fun and excitement to the conference while highlighting the importance of efficient typing in cybersecurity.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Egor's Keyboard Corner
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Keyboard Corner hosts typing challenges that test the speed and accuracy of attendees' typing skills on various keyboards. Participants can compete for high scores and bragging rights in a friendly and competitive setting. This activity adds an element of fun and excitement to the conference while highlighting the importance of efficient typing in cybersecurity.

Return to Index - Add to Google - ics Calendar file

Title: Election 2024 Freedom of Choice: A Psybernomic Conundrum
When: Friday, Aug 9, 14:00 - 14:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

This presentation delves into the geopolitical landscape of the United States and beyond, providing a critical examination of the evolving societal attitudes toward democracy, globalism, and privacy. Through the lens of psychological influence and cognitive security, we explore how cyber and economic warfare shape human behavior and decision-making processes. By bringing awareness to the myriad forces that drive individual choices—from mundane daily activities like selecting breakfast to significant actions such as voting in elections—we aim to elucidate the intricate web of influence. This includes an analysis of historical strategies employed in influence campaigns and a critical look at the technical and non-technical tactics used today. We highlight the economic underpinnings and financial mechanisms that support these campaigns, revealing the sophisticated interplay between economic warfare and psychological manipulation. Through this exploration, we seek to equip participants with a deeper understanding of the strategies behind modern influence campaigns and their profound impact on both individual and collective decision-making within democratic societies.

Speakers: Hallie Stern,Tina Schneibs

SpeakerBio: Hallie Stern

Hallie Stern is an Information Scientist specializing in emerging technology and psyber security, investigating how behavioral data shapes digital interactions and influences offline responses. Her interdisciplinary expertise spans digital humanities, algorithmic modeling, and global media, with a focus on identifying technical vulnerabilities in the information landscape.Hallie earned a B.A. in Integrative Media Studies from The University of Redlands and an M.S. in Global Security, Conflict, and Cybercrime from NYU. Her leadership extends to conducting workshops at esteemed events such as The Nobel Prize Summit, UNGA, Harvard University, and DefCon. She currently serves as the AI and technology resident fellow at the McCain Institute in Washington DC.

SpeakerBio: Tina Schneibs

Tina Schniebs is an experienced financial risk management consultant with over 20 years of experience in financial analysis and management, IT integration, and legal investigation. Extensive experience in project management, IT project life-cycle development, strategic organization, criminal, civil, and appellate law; and a unique awareness of financial risk vectors to organizations. Tina is currently a Risk Management Consultant for Ridgeline International, Inc., advising commercial, IC and DOD customers on global financial and regulatory risks to their organizations.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Embedded CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Embedded systems are everywhere in our daily lives, from the smart devices in our homes to the systems that control critical infrastructure. These systems exist at the intersection of hardware and software, built to accomplish a specific task. However, unlike general-purpose computers, embedded systems are typically designed for a particular case of use and have limited resources. This makes them both challenging and fascinating to work with, especially from a security perspective. Often these disciplines are dealt with individually, but understanding the custom relationships between hardware and software is vital to performing security research on these devices.

The embedded device CTF contest is an exciting opportunity to explore the intricacies of these systems and test your skills in a competitive environment. Contestants are challenged to find vulnerabilities in the firmware or hardware and exploit them to gain access or control over the device. The contest offers a unique opportunity to explore embedded devices' inner workings and understand their design's security implications.

New devices will be dramatically introduced at set intervals throughout the competition, and point values will decrease over time. This keeps contestants guessing and on their toes, forcing them to adapt and use their skills to tackle new challenges. It also offers a chance to learn about different types of devices and how they function, broadening participants' knowledge and experience.

By participating in the contest, contestants can develop a deep understanding of how these systems operate and how to secure them against potential attacks. Additionally, the contest encourages participants to think outside the box and approach problems creatively, honing their problem-solving skills. The competition provides a valuable opportunity to network with like-minded individuals and a chance to learn from others in the field hands-on.

Overall, the embedded device CTF contest is an exciting and educational experience that showcases the unique challenges and rewards of working with embedded devices. With the rise of the Internet of Things and the increasing integration of technology in our daily lives, embedded devices are becoming more ubiquitous, making this contest relevant and worth checking out. Whether you're a seasoned security professional or just starting in the field, the contest offers a chance to learn, test your skills, and have fun in a dynamic and competitive environment.

This is the main event at Embedded Systems Village. Come and show off your skills at hacking our collection of vulnerable embedded devices and find flags to score points! New this year we have a 101 track where each team will have their own set of emulated devices, as well as embedded challenges from the MITRE eCTF and some boss-level embedded challenges from Toyota Tsusho Systems US!

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Embedded CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Embedded systems are everywhere in our daily lives, from the smart devices in our homes to the systems that control critical infrastructure. These systems exist at the intersection of hardware and software, built to accomplish a specific task. However, unlike general-purpose computers, embedded systems are typically designed for a particular case of use and have limited resources. This makes them both challenging and fascinating to work with, especially from a security perspective. Often these disciplines are dealt with individually, but understanding the custom relationships between hardware and software is vital to performing security research on these devices.

The embedded device CTF contest is an exciting opportunity to explore the intricacies of these systems and test your skills in a competitive environment. Contestants are challenged to find vulnerabilities in the firmware or hardware and exploit them to gain access or control over the device. The contest offers a unique opportunity to explore embedded devices' inner workings and understand their design's security implications.

New devices will be dramatically introduced at set intervals throughout the competition, and point values will decrease over time. This keeps contestants guessing and on their toes, forcing them to adapt and use their skills to tackle new challenges. It also offers a chance to learn about different types of devices and how they function, broadening participants' knowledge and experience.

By participating in the contest, contestants can develop a deep understanding of how these systems operate and how to secure them against potential attacks. Additionally, the contest encourages participants to think outside the box and approach problems creatively, honing their problem-solving skills. The competition provides a valuable opportunity to network with like-minded individuals and a chance to learn from others in the field hands-on.

Overall, the embedded device CTF contest is an exciting and educational experience that showcases the unique challenges and rewards of working with embedded devices. With the rise of the Internet of Things and the increasing integration of technology in our daily lives, embedded devices are becoming more ubiquitous, making this contest relevant and worth checking out. Whether you're a seasoned security professional or just starting in the field, the contest offers a chance to learn, test your skills, and have fun in a dynamic and competitive environment.

This is the main event at Embedded Systems Village. Come and show off your skills at hacking our collection of vulnerable embedded devices and find flags to score points! New this year we have a 101 track where each team will have their own set of emulated devices, as well as embedded challenges from the MITRE eCTF and some boss-level embedded challenges from Toyota Tsusho Systems US!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Embedded CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Embedded systems are everywhere in our daily lives, from the smart devices in our homes to the systems that control critical infrastructure. These systems exist at the intersection of hardware and software, built to accomplish a specific task. However, unlike general-purpose computers, embedded systems are typically designed for a particular case of use and have limited resources. This makes them both challenging and fascinating to work with, especially from a security perspective. Often these disciplines are dealt with individually, but understanding the custom relationships between hardware and software is vital to performing security research on these devices.

The embedded device CTF contest is an exciting opportunity to explore the intricacies of these systems and test your skills in a competitive environment. Contestants are challenged to find vulnerabilities in the firmware or hardware and exploit them to gain access or control over the device. The contest offers a unique opportunity to explore embedded devices' inner workings and understand their design's security implications.

New devices will be dramatically introduced at set intervals throughout the competition, and point values will decrease over time. This keeps contestants guessing and on their toes, forcing them to adapt and use their skills to tackle new challenges. It also offers a chance to learn about different types of devices and how they function, broadening participants' knowledge and experience.

By participating in the contest, contestants can develop a deep understanding of how these systems operate and how to secure them against potential attacks. Additionally, the contest encourages participants to think outside the box and approach problems creatively, honing their problem-solving skills. The competition provides a valuable opportunity to network with like-minded individuals and a chance to learn from others in the field hands-on.

Overall, the embedded device CTF contest is an exciting and educational experience that showcases the unique challenges and rewards of working with embedded devices. With the rise of the Internet of Things and the increasing integration of technology in our daily lives, embedded devices are becoming more ubiquitous, making this contest relevant and worth checking out. Whether you're a seasoned security professional or just starting in the field, the contest offers a chance to learn, test your skills, and have fun in a dynamic and competitive environment.

This is the main event at Embedded Systems Village. Come and show off your skills at hacking our collection of vulnerable embedded devices and find flags to score points! New this year we have a 101 track where each team will have their own set of emulated devices, as well as embedded challenges from the MITRE eCTF and some boss-level embedded challenges from Toyota Tsusho Systems US!

Return to Index - Add to Google - ics Calendar file

ESV - Friday - 10:00-17:59 PDT

Title: Emulating (and Hacking) Embedded Devices
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Hack your first embedded system! Sit down at our provided laptops and be guided through exploiting an IP camera, then learn how you can set up the emulated camera (and other devices) at home with Ludus!

Return to Index - Add to Google - ics Calendar file

ESV - Sunday - 10:00-12:59 PDT

Title: Emulating (and Hacking) Embedded Devices
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Hack your first embedded system! Sit down at our provided laptops and be guided through exploiting an IP camera, then learn how you can set up the emulated camera (and other devices) at home with Ludus!

Return to Index - Add to Google - ics Calendar file

ESV - Saturday - 10:00-17:59 PDT

Title: Emulating (and Hacking) Embedded Devices
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Hack your first embedded system! Sit down at our provided laptops and be guided through exploiting an IP camera, then learn how you can set up the emulated camera (and other devices) at home with Ludus!

Return to Index - Add to Google - ics Calendar file

PYV - Friday - 14:30-15:10 PDT

Title: Emulating Magstripe with Arduino
When: Friday, Aug 9, 14:30 - 15:10 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

Learn how to build a device to emulate magstripe using data intercepted from EMV chip and contactless interfaces

SpeakerBio: Leigh-Anne Galloway, Director of Research at UNDERLE LTD

Leigh-Anne Galloway is the Payment Village Lead and Director of Research at UNDERLE LTD. Leigh-Anne started her career in incident response, leading investigations into payment card data breaches. This is where she discovered her passion for security advisory and payment technologies. She authored research on ATM security, application security and payment technology vulnerabilities; and has previously spoken at DevSecCon, BSides, Hacktivity, 8dot8, OWASP, and Troopers, Black Hat USA, Black Hat Europe and DEF CON. She also serves on the board for Black Hat Europe.

Return to Index - Add to Google - ics Calendar file

PYV - Saturday - 11:30-12:10 PDT

Title: Emulating Magstripe with Arduino
When: Saturday, Aug 10, 11:30 - 12:10 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

Learn how to build a device to emulate magstripe using data intercepted from EMV chip and contactless interfaces

SpeakerBio: Leigh-Anne Galloway, Director of Research at UNDERLE LTD

Leigh-Anne Galloway is the Payment Village Lead and Director of Research at UNDERLE LTD. Leigh-Anne started her career in incident response, leading investigations into payment card data breaches. This is where she discovered her passion for security advisory and payment technologies. She authored research on ATM security, application security and payment technology vulnerabilities; and has previously spoken at DevSecCon, BSides, Hacktivity, 8dot8, OWASP, and Troopers, Black Hat USA, Black Hat Europe and DEF CON. She also serves on the board for Black Hat Europe.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 16:00-16:45 PDT

Title: Encrypted newspaper ads in the 19th century - The world's first worldwide secure communication system
When: Saturday, Aug 10, 16:00 - 16:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

Between 1850 and 1855, the London-based newspaper The Times published over 50 encrypted advertisements apparently intended for the same recipient. As we know today, the ads in that series were meant for the sea captain Richard Collinson, who at the time was on a mission in the Canadian Arctic trying to solve a captivating mystery: What happened to the lost John Franklin expedition? While Collinson never reached his goal, he established a secure worldwide communication system, which was unique for its time.

Before his departure, Collinson's family was taught how to encrypt brief reports about what was going on at home and to publish these messages as mysterious ads in “The Times” once a month. The cipher used was a modified version of a system based on a signal-book of the Royal Navy. As the circulation of The Times stretched far beyond the UK, Collinson would have the chance to get his hands on a copy even at the remotest of ports.

Over a century later, the Collinson ads were finally broken in the 1990s. Over the last two years, the lecturers of this talk continued this work, with a goal of decrypting all of the ads and placing them in their appropriate geographic and cultural context.

- Article in “Mental Floss” (this was written based on one of our earlier talks)
    - Ellen Gutoskey: How Victorian Explorers and Pining Lovers Used Coded Newspaper Ads to Communicate. Aug 10, 2022
    - link
- 1992 Research paper in Cryptologia:
    - John Rabson: All are Well at Boldon a mid-Victorian Code System. Cryptologia 16(2): 127-135 (1992)
- Book about encrypted newspaper advertisements:
    - Jean Palmer: The Agony Column Codes & Ciphers. New Generation Publishing, London 2006
- Naval codebooks:
    - 10th edition (1847): link
    - 11th edition (1851): link
    - 12th edition (1854): link
- Collinson’s logbooks (by his brother):
    - Thomas Bernard Collinson: Cypher Notices in the ‘Times’. In: Journal of H.M.S. Enterprise, on the Expedition in Search of Sir John Franklin's Ships by Behring Strait. 1850-55. Sampson Low, Marston, Searle, & Rivington. London: 1889 link
- Article from the 1940s:
    - Richard J. Cyriax: The Collinson Cryptograms in "The Times". Notes and Queries 26 July, 1947: 322-323

Speakers: Elonka Dunin,Klaus Schmeh

SpeakerBio: Elonka Dunin, Crypto Expert

Elonka Dunin is a crypto expert and co-leader of a group that is working to crack the final cipher on the Kryptos sculpture at CIA Headquarters. She maintains a website of the World's most famous unsolved codes, and bestselling author Dan Brown named his character "Nola Kaye", a scrambled form of "Elonka", in his novel The Lost Symbol, after her.

Elonka was a member of the Board of Directors for the National Cryptologic Museum Foundation, and General Manager and Executive Producer at Simutronics, making award-winning online and mobile games.

In 2006, Elonka published The Mammoth Book of Secret Codes and Cryptograms, and with Klaus she co-wrote the book Codebreaking: A Practical Guide, with editions in 2020 and 2023.

SpeakerBio: Klaus Schmeh, Crypto Expert at Eviden

Klaus Schmeh has written 15 books (mostly in German) about cryptography, as well as over 250 articles, 25 scientific papers, and 1500 blog posts. Klaus's main fields of interest are codebreaking and the history of encryption.

Klaus is a popular speaker, known for his entertaining presentation style involving self-drawn cartoons, self-composed songs, and Lego models. He has lectured at hundreds of conferences, including the NSA Crypto History Symposium, DEF CON, and the RSA Conference.

In his day job, Klaus works as a crypto expert for the global IT security company Eviden.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 14:40-15:10 PDT

Title: Engineers & Exploits: The Quest for Security
When: Saturday, Aug 10, 14:40 - 15:10 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Efficient threat modelling is essential for finding and fixing vulnerabilities. Yet empowering threat modelling trainers to communicate in a way that ensures actionable solutions, moving beyond the directive to “fix SQLI.” is a common challenge. This talk presents strategies for training threat modelers, ensuring they can communicate techniques and principles needed to better and address vulnerabilities early on in the SDLC

Introducing: "Engineers & Exploits: The Quest for Security" a derivative of the Cornucopia card game. While Cornucopia is an excellent introductory threat modelling exercise, we found limitations when training our coworkers to subsequently instruct developers. To bridge this gap, we developed a tabletop game designed to improve the learning experience. In this interactive session, we will show game mechanics and explain benefits, Join us to discover how you can transform threat modelling education, making it engaging for trainers and trainees.

Speakers:
Andra,Spyros Gasteratos

SpeakerBio: Andra

Andra is a Principal Application Security Specialist at Sage, with over seven years of experience in the field of application security. She is responsible for implementing DevSecOps practices, conducting security assessments, and developing secure coding guidelines for software engineering and AI/ML teams. She holds multiple certifications, including AWS Certified Cloud Practitioner and Attacking and Securing APIs. She has a strong background in software development and project management, as well as a master's degree in information and computer sciences. She has been co-leading the OWASP London Chapter since 2019, where she organises and delivers events and workshops on various security topics. She is passionate about educating and empowering developers and stakeholders to build and deliver secure software and best practices in a fast-paced, results-driven environment.

SpeakerBio: Spyros Gasteratos

Spyros has over 15 years of experience in the security world. Since the beginning of his career he has been an avid supporter and contributor of open source software and an OWASP volunteer. Currently he is interested in the harmonization of security tools and information and is currently helping Fintechs setup and automate large parts of their AppSec programmes. He also maintains several Open Source projects including the security automation framework Dracon, and opencre.org, the worlds largest security knowledge graph. Also, he usually doesn’t speak about himself in the third person.

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 15:10-15:40 PDT

Title: Epyon - Attacking DevOps environments
When: Friday, Aug 9, 15:10 - 15:40 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

A CI/CD pipeline is a sequence of steps designed to automate the software delivery process. DevOps environments consist of multiple systems that collaborate to facilitate CI/CD pipelines. However, DevOps systems are significant targets for attackers due to their possession of credentials and access keys for various components, including domain accounts, databases, and cloud assets. Epyon is a versatile tool for red teamers to target common DevOps systems. It is open source and written entirely in Golang. Moreover, it features multiple modules, such as GitLab, SonarQube, and Azure DevOps. During this demonstration, I will present examples (based on real project experiences) of how to utilize Epyon for privilege escalation and lateral movement within a DevOps environment.

SpeakerBio: Victor Pasknel

Cybersecurity professional with a proven track record of 13 years in executing red-team operations, penetration testing, war games, and vulnerability assessments. Possessing a strong academic background, including a PhD in Applied Informatics from the University of Fortaleza (Brazil) earned in 2022, coupled with over a decade of experience as a university professor specializing in information security.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 16:00-16:45 PDT

Title: Eradicating Hepatitis C With BioTerrorism
When: Friday, Aug 9, 16:00 - 16:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

A quarter of a million people die from Hepatitis C every year. Fifty million people are currently infected, and a million more are infected each year. But for the first time in history there is a cure (not just a treatment) for a virus, and it is for Hepatitis C. Take one 400mg pill of Sofosbuvir every day for twelve weeks, and you will be free of the virus. The catch? Those pills are one thousand US dollars apiece because the molecule is the "Intellectual Property" of Gilead Pharmaceuticals, and they refuse to share. So if you have $84,000 USD, Hep C is not your problem. But for everyone else, The Four Thieves Vinegar Collective has developed a way to make the entire course of treatment for $300 USD. This methodology also applies to other diseases. Like any science, the method of manufacture of drugs can be replicated, and we are going to give you all the necessary tools and show you the process top-to-bottom. Watch it happen live, participate, and learn to do it yourself: Use our digital research assistant to help you navigate the scientific literature, feed your medicine of choice into ChemHacktica to get a chemical synthesis pathway, put that procedure into the Recipe Press to generate code for the new version of the MicroLab to run, and watch the medicine form in the reaction chamber. Finally come on stage, press some tablets, and make your own thousand-dollar pill for four dollars in materials. The feds say saving a life this way is bioterrorism. We say: So Be It.

SpeakerBio: Mixæl Swan Laufer, Chief Spokesperson at Four Thieves Vinegar Collective

Mixæl Swan Laufer worked in mathematics and high energy physics until he decided to use his background in science to tackle problems of global health and human rights. He now is the chief spokesperson for the Four Thieves Vinegar Collective which works to make it possible for people to manufacture their own medications and medical devices at home by creating public access to tools, ideas, and information.

Return to Index - Add to Google - ics Calendar file

BHV - Saturday - 11:00-11:59 PDT

Title: Eradicating Hepatitis C With BioTerrorism
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

A quarter million people die from Hepatitis C yearly, and it's getting worse. But for the first time in history there is a cure (not just a treatment) for a virus, and it is for Hepatitis C. Take one 400mg pill of Sofosbuvir every day for twelve weeks, and you will be free of the virus. The catch? Those pills are $1,000 USD apiece because the molecule is the so-called "Intellectual Property" of Gilead Pharmaceuticals, and they refuse to share. If you have $84,000 USD, Hep C is not your problem. We have developed a way to make the entire course of treatment for $300 USD. This methodology also applies to other diseases. Like any science, the method of manufacture of drugs can be replicated, and we are going to give you all the necessary tools and show you the process top-to-bottom. Watch it happen live, participate, and learn to do it yourself: Use our digital research assistant to help you navigate the scientific literature, get a chemical synthesis pathway, generate code for the the MicroLab to run, and watch the medicine form in the reaction chamber. Finally, press some tablets. The feds say saving a life this way is BioTerrorism. We say: So Be It.

SpeakerBio: Mixæl Swan Laufer, Chief Spokesperson at Four Thieves Vinegar Collective

Mixæl Swan Laufer worked in mathematics and high energy physics until he decided to use his background in science to tackle problems of global health and human rights. He now is the chief spokesperson for the Four Thieves Vinegar Collective which works to make it possible for people to manufacture their own medications and medical devices at home by creating public access to tools, ideas, and information.

Return to Index - Add to Google - ics Calendar file

AIxCC - Saturday - 14:30-14:59 PDT

Title: Establishing the first Open Source Program Office at a United States Federal Agency
When: Saturday, Aug 10, 14:30 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Open Source Program Offices (OSPOs) are an increasingly adopted approach to establishing and cultivating a culture of contribution. The Digital Service at CMS.gov will share the programs, policies, and projects they're building to identify and mitigate continuity and security risks in the software supply chain across the Federal Ecosystem.

SpeakerBio: Remy DeCausemaker, Open Source Lead at Center for Medicare and Medicaid Services

Wearing the Suit so Hackers don't have to.

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 11:00-11:30 PDT

Title: Evading Modern Defenses When Phishing with Pixels
When: Saturday, Aug 10, 11:00 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Dive into the art of phishing with QR codes! We'll cover the fundamentals of QR code phishing, revealing how these innocuous-looking images are used to deceive users into a false sense of legitimacy. After touching upon the basics, we'll explore creative tactics for obfuscating and hiding QR codes to ensure they reach their intended targets. As a sidetrack, we'll delve into how emails are rendered within the Outlook Mail Application and showcase some neat tricks that exploit its limitations for hiding QR codes from modern defensive solutions. Overall, the talk is intended to help testers up their QR code phishing game!

SpeakerBio: Melvin Langvik, Offensive Security Team Lead at Kovert AS

Melvin Langvik is an accomplished professional with a diverse background in technology. He started his career as a developer and integration consultant, where he gained practical experience in developing and distributing critical backend infrastructure for an international customer base.

Melvin's passion for cybersecurity later led him to transition into offensive security. He previously worked for TrustedSec, an internationally recognized security company. Melvin was a part of TrustedSec's targeted operations team, tasked with performing targeted cyber attacks against some of the most mature and often largest companies in the world. Today, Melvin is the Offensive Security Team Lead at Kovert AS.

Return to Index - Add to Google - ics Calendar file

AIV - Saturday - 14:30-14:59 PDT

Title: Evaluations and Guardrails against Prompt Injection attacks on LLM powered-applications
When: Saturday, Aug 10, 14:30 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Prompt injections are a class of attacks against LLM-powered applications that exploit the inclusion of untrusted user inputs in LLM prompts. We give an overview of two open source frameworks developed by Meta related to understanding and mitigating prompt injection risks:

- our CyberSecEval Prompt Injection benchmarks (evaluations of the propensity of popular LLMs to succumb to prompt injection when used without guardrails),
- as well as PromptGuard (an open-source model for identifying risky inputs to LLM-powered applications, both direct jailbreaks and indirect injections).

Findings of interest:

- Evaluating foundation model vulnerability to indirect prompt injection: LLMs can be trained to have contextual awareness of which parts of the input prompt are coming from a trusted user versus an untrusted third party - in particular via inclusion of a system prompt. We share our benchmark for direct and indirect prompt injection susceptibility of foundational LLMs (across a wide variety of attack strategies) introduced as part of CyberSecEval (an open-source suite of benchmarks for measuring the cybersecurity risks of foundational models). We present the results of these evaluations for currently-popular foundational LLMs. We conclude that model conditioning is not enough to defend against indirect prompt injection risks in most contexts, even with the usage of a system prompt.
- Guardrailing against prompt injection attacks in real applications: We present PromptGuard, a model designed for both the detection of direct jailbreak and indirect injection attacks. We highlight the differences between our models and existing malicious prompt detectors (which largely only address direct prompt injection or jailbreaking risks), and the specific risks that can be prevented by utilizing our guardrail in LLM-powered applications. We also show how the model can be fine-tuned to improve application-specific performance.

Speakers: Cyrus Nikolaidis,Faizan Ahmad

SpeakerBio: Cyrus Nikolaidis, Meta Platforms, Inc.
No BIO available
SpeakerBio: Faizan Ahmad, Meta Platforms, Inc.
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Evolution of RF Signal Visualization - From Spectrum Analyzers to Augmented Reality
When: Sunday, Aug 11, 10:00 - 10:30 PDT
Where: Other / See Description

Description:

We are surrounded by invisible radio frequency signals created by human technology like radio, cellular, and satellite. Traditionally, we see these signals through spectrum analyzers. However, the capabilities of existing analysis tools are being outpaced by the rapid modernization of wireless networks and topologies like 5G, IoT, Bluetooth, LoRa, etc. RF is inherently multidimensional, but conventional analyzers display signals in 2D slices, limiting real-world applicability to highly technical users. Emerging technology that combines Augmented Reality displays and AI/ML algorithms is capable of spatializing RF data into its natural 3D location for easier understanding and communication.

This talk will provide an overview of the evolution of RF visualization tools from flat interfaces to immersive ones that can be used to discover and map RF signals and networks. The audience will gain a broad understanding of the emergence of immersive interfaces and how they can be applied successfully to spatial data visualization. We will walk participants through challenges with the design and development process, theory behind decisions, and usability issues to overcome in actual deployments. Resulting best practices will be shared openly. Finally, the audience will learn about future applications of these tools and forecasted innovations as the underlying technology matures.

Speakers: Suzanne Borders,Jad Meouchy

SpeakerBio: Suzanne Borders, Founder and CEO at BadVR

Suzanne studied psychology at University of Missouri, Kansas City and previously worked as Lead UX/Product Designer for over 9 years at companies such as Remine (raised $48M) and CREXi (raised $54M) where she specialized in designing intuitive, high-performant data analytic interfaces. In 2019, Suzanne founded BadVR and was awarded a “Rising Stars” innovation award from IEEE. To date, she’s raised over $4M in non-dilutive funding for BadVR, via grants from the National Science Foundation, NOAA, Magic Leap, Qualcomm, and more. Suzanne has grown the company from 2 to 25 people and was awarded 4 patents for innovations she created while leading the BadVR team.

Over the past 5 years, Suzanne emerged as a thought-leader in the immersive data visualization and analytics space. She has been a keynote speaker at over 25 national and international conferences. In her spare time, Suzanne travels for inspiration (81 countries and counting) and is proud to be a published author and former punk. Suzanne thrives at the intersection of product design, immersive technology, and data; she’s a believer in the artistry of technology and the technicality of art and remains passionately dedicated to democratizing access to data through universally accessible products.

SpeakerBio: Jad Meouchy, Co-Founder and CTO at BadVR

Jad Meouchy, CTO + Co-Founder, BadVR, Inc. Jad, originally from northern Virginia, holds dual B.S. degrees in Computer Engineering and Psychology from Virginia Tech, and is a graduate of the Thomas Jefferson High School for Science and Technology. While in college, he engineered and built the data visualization components of an emergency response simulation that went on to receive 2M in public grant funding. Over his 15-year career, Jad has founded five startups and successfully exited three. His professional expertise is in software architecture and development, specifically big data analytics and visualization, and virtual and augmented reality development. Based in Los Angeles since 2010, Jad promotes the community by organizing developer meetups and events, and volunteering time for STEM initiatives.

Return to Index - Add to Google - ics Calendar file

BICV - Sunday - 13:00-13:59 PDT

Title: Expanding Pathways into the National Cyber Workforce
When: Sunday, Aug 11, 13:00 - 13:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

The nation is facing a shortage of approximately 500,000 good paying jobs in cyber.The problem is only going to continue to grow as the world becomes more digitized. This is a threat to our national security. The White House Office of the National Cyber Director (ONCD) is ensuring that as we build the cyber workforce the nation needs, we are reaching out to every community. Diversity is an essential element of the national cyber workforce. National Cyber Director (NCD) Harry Coker Jr., and his predecessor Kemba Walden, have both been leading our work to build the nations cyber workforce, one that is reflective of nation and its needs.

SpeakerBio: Ayan Islam, ONCD, White House

Ayan Islam, a Somali native, is a key member of the ONCD team who handles workforce outreach to the African American Community, HBCU's and many diverse audiences the nation desperately needs to assist with our national security. During this session, she will recount her experience, extensive background and her work with senior leaders. She will focus on ONCD's work to expand pathways for individuals from backgrounds that are currently underrepresented in the Federal and national cyber workforce, including African Americans, to launch good-paying, meaningful careers in the cyber workforce.

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 13:25-13:59 PDT

Title: Exploit K8S via Misconfiguration .YAML in CSP environments
When: Friday, Aug 9, 13:25 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

In this presentation, we researched vulnerable security configurations that enable attacks on Kubernetes (K8s) clusters and examined how these settings can be exploited in CNCF projects. Kubernetes (K8s) uses YAML files to manage various security settings, leading to potential attacks such as information leakage, excessive permission acquisition, and container escape.

Initially, this study focused on three security configuration areas in K8s: RBAC, HostPID, and Security Context. We explained the threats present if vulnerable settings are included.

```
- RBAC: Excessive permission in K8s resources allows sensitive information theft or access to other
- HostPID: Access to node process information enables container escape attacks
- Security Context: Incorrect security settings enable node escape and host access
```

Next, we created patterns for identifying weak security settings through YAML files. To do this, we conducted a literature review and expanded the vulnerable patterns centered on RBAC proposed in various papers. Additionally, we included other security settings (HostPID, Security Context). [Our Pattern vs Paper Pattern]

```
1. RBAC:
    - Our: Daemonset, Deployment SA > node Patch and Secret Get/List
    - Paper: Daemonset > node Patch and Secret Get/List
2. Kind:
    Our: Cluster Role, Role, Role Binding
    Paper: Cluster Role
3. Other Security configurations:
    - Our: HostPID, SecurityContext
    - Paper: X
```

Utilizing these patterns, we examined over 150 widely-used 3rd-party CNCF projects in K8s, discovering more than 50 instances of vulnerable patterns. We provide detailed demonstrations of three scenarios for seizing nodes or clusters by using the discovered patterns to set Base Attack conditions.

[Base Attack Conditions]

```
- RBAC > Demonset / Deployment > Service Account > Secret (Get/List) or Node(Patch)
[Exploit Scenario]
- Stealing Tokens using Pods with excessive privileges
- Node Take over via 1 Day (CVE-2022-42889) or hostPID: True or Security Context
- Take over of another node or cluster using the Service Account Token on the deodorized node
```

Additionally, we are aware that 3rd-Party CNCF projects are widely used for convenience when operating K8S in CSPs (AWS, Azure, GCP). Since scenarios can occur in a CSP environment, we demonstrate in more detail. Finally, based on these research results, we share vulnerable patterns with project owners to collaborate on patching and issue tracking. Before the presentation, we plan to share any reporting on CVEs and patch notes.

Speakers:
Wooseok Kim,Changhyun Park

SpeakerBio:
Wooseok Kim

Wooseok Kim - Goorm | Site Reliability Engineer | K8S, CSP | SKKU

SpeakerBio: Changhyun Park

Changhyun Park - MatchGroup | Hyperconnect | Security Compliance Analyst | Cloud, GRC | SKKU

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 13:00-13:25 PDT

Title: ExploitIfNotExists: Privilege Escalation & Persistence with Azure Policy
When: Friday, Aug 9, 13:00 - 13:25 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

The Microsoft Azure threat matrix contains a mysterious and almost empty item: AZT508 - Azure Policy, which suggests this service can break bad but gives almost no details as to how. To quote Microsoft: “Azure Policy helps to enforce organizational standards and to assess compliance at-scale.“ How does this banal sounding service come to be used for attacking Azure users?

This talk aims to fill in the picture. We will explore the Azure Policy service and how it can be used for badness: punching holes in acls, creating persistent backdoors on virtual machines, assigning attacker controlled roles to resources, modifying database encryption, etc. I will demo an abuse scenario, and discuss others that can be used for privilege escalation and persistence. I will also discuss a confused deputy attack on this service. Finally, I will share detection and control recommendations.

Talk Outline:

The Azure Policy service (3 mins): - What it is, how it works, and how it is intended to be used. This service is billed as an integral part of the Azure compliance story. Policies examine resources and can block or alert on non-compliance. - Introduce the components at play and lay the groundwork for understanding later abuse. -----There are lots of interlocking pieces to understand. - Introducing policy effects which go far beyond normal auditing scope. Effects are how policies can make changes to resource configuration.

Establishing the abuse case: (7 mins) - Discussion of evil that can be done with intended functionality including a demo - Policy adds an arbitrary script to every VM, which runs as soon as it starts up, calling a reverse shell home. - Policy turns off database encryption - Policy to assign an RBAC role to attacker controlled account - What privileges and roles are need for the above

Privesc scenario (7 mins) - Policy initiatives - these are higher level groupings of policies - Confused deputy attack via initiative - The curious case of `append` actions - Policies can append an attacker IP to every new ACL in your environment - Adding attacker ssh keys to all VMs

SpeakerBio: Zander Mackie

Zander Mackie is a father, husband, security researcher, and developer. He’s worked across the stack as a software engineer, from fixing CSS bugs to writing systems code for container orchestration. He’s driven by a relentless need to figure out how things work and fixing bugs is his favorite.

Return to Index - Add to Google - ics Calendar file

CHV - Saturday - 16:00-16:30 PDT

Title: Exploiting Bluetooth - from your car to the bank account$$
When: Saturday, Aug 10, 16:00 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Over the past decade, infotainment systems experienced a growth in functionality, broader adoption and central incorporation into the vehicle architecture. Due to the ever-growing role of wireless protocols such as Bluetooth and a known lack of patches alongside the difficulty of patch installation, this poses a new attack surface and a genuine threat to the users. At the same time, the tools and methodologies required for testing are scattered across the Internet, absent and need a rigorous setup.

In this talk, we share a comprehensive framework BlueToolkit to test and replay Bluetooth Classic vulnerabilities. We provide practical information and tips. Additionally, we release new exploits and a privilege escalation attack vector.

We show how we used the toolkit to find 64 new vulnerabilities in 22 modern cars and the Garmin Flight Stream flight management system used in several aircraft types.

Our work equips Bluetooth hackers with necessary information on novel implementation-specific vulnerabilities that could be used to steal information from target cars, establish MitM position or escalate privileges to hijack victims' accounts stealthily.

We believe our research will be beneficial in finding new vulnerabilities and making Bluetooth research more accessible and reproducible.

Speakers: Vladyslav Zubkov,Martin Strohmeier

SpeakerBio: Vladyslav Zubkov, Bug Bounty Hunter

Vladyslav Zubkov (aka yso and schwytz) is a bug bounty hunter. He is consistently among the top hackers at live hacking events organized by Meta, Intel, Louis Vuitton, Intigriti and YesWeHack. His interests include vulnerability research, application security, red teaming, bug bounty hunting, developing tools and proactively securing systems.

SpeakerBio: Martin Strohmeier, Senior Scientist at Cyber Defence Campus

Martin Strohmeier is a Senior Scientist at the Swiss Cyber Defence Campus, where he is responsible for vulnerability research programmes into aircraft, satellites and cars. His work was published in all major systems security conferences, totalling more than 100 publications to date. He has also spoken previously at the DEFCON Aerospace Village and co-organized CTFs there.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 17:30-18:15 PDT

Title: Exploiting Bluetooth - from your car to the bank account$$
When: Friday, Aug 9, 17:30 - 18:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Over the past decade, infotainment systems have experienced a growth in functionality, broader adoption, and central incorporation into vehicle architecture. Due to the ever-growing role of wireless protocols such as Bluetooth and a known lack of patches alongside the difficulty of patch installation, this poses a new attack surface and a genuine threat to the users. Meanwhile, the tools and methodologies required for testing are scattered across the Internet, absent and need a rigorous setup.

In this talk, we share a comprehensive framework BlueToolkit to test and replay Bluetooth Classic vulnerabilities. Additionally, we release new exploits and a privilege escalation attack vector.

We show how we used the toolkit to find 64 new vulnerabilities in 22 modern cars and the Garmin Flight Stream flight management system used in several aircraft types. Our work equips hackers with insights and necessary information on novel vulnerabilities that could be used to steal information from target cars, establish MitM position or escalate privileges to hijack victims' accounts and MFA codes stealthily.

Overall, we show vulnerabilities in cars, aircraft and smartphones. We believe our research will be beneficial in finding new vulnerabilities and making Bluetooth research more accessible and reproducible.

References:

- BlueToolkit - Bluetooth Classic vulnerability testing framework link (all exploits will be uploaded after 9th of August)
- MapAccountHijack - Tool that allows hijacking services by exploiting widely used Bluetooth Classic functionality link - link (accessible after 9th of August)
- D. Antonioli and M. Payer. On the insecurity of vehicles against protocol-level bluetooth threats. In 2022 IEEE Security and Privacy Workshops (SPW), pages 353–362, Los Alamitos, CA, USA, May 2022. IEEE Computer Society.
- Cross-Sectional Analysis of the Bluetooth Stack of Modern Cars - (The link will be updated)
- Wenjian Xu. Stealthily Access Your Android Phones: Bypass The Bluetooth Authentication. link, 2020.
- Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. Blue's clues: Practical discovery of non-discoverable bluetooth devices. In 2023 IEEE Symposium on Security and Privacy (SP), pages 3098–3112, 2023.
- Maximilian von Tschirschnitz, Ludwig Peuckert, Fabian Franzen, and Jens Grossklags. Method confusion attack on bluetooth pairing. In 2021 IEEE Symposium on Security and Privacy (SP), pages 1332–1347, 2021.
- Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR. In USENIX Security Symposium (SEC), August 2019

Speakers: Vladyslav Zubkov,Martin Strohmeier

SpeakerBio: Vladyslav Zubkov, Bug Bounty Hunter

Vladyslav Zubkov (aka yso and schwytz) is a bug bounty hunter. He is consistently among the top hackers at live hacking events organized by Meta, Intel, Louis Vuitton, Intigriti and YesWeHack. His interests include vulnerability research, application security, red teaming, bug bounty hunting, developing tools and proactively securing systems.

SpeakerBio: Martin Strohmeier, Senior Scientist at Cyber Defence Campus

Martin Strohmeier is a Senior Scientist at the Swiss Cyber Defence Campus, where he is responsible for vulnerability research programmes into aircraft, satellites and cars. His work was published in all major systems security conferences, totalling more than 100 publications to date. He has also spoken previously at the DEFCON Aerospace Village and co-organized CTFs there.

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 16:00-17:59 PDT

Title: Exploiting common vulnerabilities in AWS environments
When: Saturday, Aug 10, 16:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Whether you are responsible for attacking or defending cloud environments, you want to know how attackers compromise them and what successful post-exploitation looks like in the cloud.

This workshop focuses on learning how attackers typically compromise cloud environments, and what post-exploitation looks like. Each workshop attendee will have access to an AWS account deployed with a collection of intentionally vulnerable cloud resources that represent misconfigurations exploited during real cloud penetration tests.

In most cases, attackers gain initial access to cloud environments in one of three ways: They compromise a vulnerable application or service in the cloud, a misconfigured cloud resource, or a user with access to the cloud. In this workshop we will be attacking an intentionally vulnerable cloud environment with all three types of vulnerabilities.

Each section of the workshop will start with an instructor led introduction followed by hands-on hacking. There is something for everyone, regardless of your offensive skill level. Anyone familiar with Linux commands and the AWS CLI is welcome to attend, and even those who have been in the field for years will find something to challenge them.

SpeakerBio: Seth Art

Seth Art is a Senior Security Advocate at Datadog. Prior to joining Datadog, Seth created and led the Cloud Penetration Testing practice at Bishop Fox. He is the author of multiple cloud focused open source tools including BadPods, IAMVulnerable, and CloudFoxable, and the co-creator of the popular cloud penetration testing tool, CloudFox.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 12:30-13:25 PDT

Title: Exploiting insecure OTA updates to create the worlds first Toothbrush Botnet and selfreplicating ESP32 worm
When: Friday, Aug 9, 12:30 - 13:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

This presentation follows the journey of investigating, conceptualizing, and implementing a Wormable Botnet for the Evowera Planck Mini Smart Manual Toothbrush, as fear-mongered by the team at Fortinet. We'll start with a high level overview of how the ESP32 OTA process works, as well as cover issues with the reference implementation released by Espressif. We'll then pivot to specifically attacking the Evowera Planck mini, dumping the firmware and doing some lite RE, monitoring the devices wireless traffic, theorizing exploits and fuzzing undocumented PCB, writing botnet software, as well as what is involved in getting an ESP32 to serve the firmware it is running as an OTA update to other Evowera Planck Minis. We'll then conclude with some proof that the devices do function as a botnet, complete with a stealthy github based C2.

SpeakerBio: Lozaning

Lozaning (they/them) has been wardriving for over 10 years and enjoys designing, building, and assembling unorthodox network observation platforms such as: The Wifydra , The International Wigle Space Balloon, and turning an Amtrak roomette into a mobile radio observation lab. Currently ranked as the 63rd best wardriver in the world on Wigle.net, Lozaning loves all things wifi and high precision GNSS related, and is starting to maybe figure out BLE.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 15:00-15:45 PDT

Title: Exploiting the Unexploitable: Insights from the Kibana Bug Bounty
When: Saturday, Aug 10, 15:00 - 15:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

aWe explore case studies of exploiting vulnerabilities in modern JavaScript and TypeScript applications, drawing on experiences from participating in the Kibana Bug Bounty Program. It's not uncommon to encounter a vulnerability that appears unexploitable at first glance, or to be told by a triage team that the behavior is "by design." So, what options does a security researcher have in such situations? And what primitives can be utilized to construct an exploitation chain with significant impact?

Our study involves breaking out of properly isolated containers in scenarios where there is RCE-by-design. We will examine several Prototype Pollutions that crash an application in less than one second after exploitation and explore how these vulnerabilities can ultimately lead to critical RCEs. Furthermore, we introduce new primitives and gadgets that enable the achievement of RCE from Prototype Pollutions previously deemed unexploitable beyond DoS attacks.

By highlighting these methods, the talk aims to equip attendees with advanced techniques for exploiting complex vulnerability chains in JavaScript applications, as well as recommendations for proper defense and mitigations against them.

1. Mikhail Shcherbakov, Musard Balliu and Cristian-Alexandru Staicu "Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js"
2. "Collection of Server-Side Prototype Pollution gadgets" link
3. Olivier Arteau "JavaScript prototype pollution attack in NodeJS"
4. Nir Chako "Attacking Kubernetes Clusters Through Your Network Plumbing" link

SpeakerBio: Mikhail Shcherbakov

Mikhail Shcherbakov came to security from enterprise app development. The tendency is to push it as far as you can… He is now doing a Ph.D. in Language-Based Security after 10+ years of experience in the industry. He participated in Microsoft, GitHub, and open-source bug bounty programs, found vulnerabilities in popular products, and helped to fix them. Before starting a Ph.D. program, he focused on .NET and web security, gave talks at conferences, organized IT meetups, and got the Microsoft MVP Award in 2016 – 2018. Mikhail is an author of commercial static analysis tools and continues research in program analysis.

Return to Index - Add to Google - ics Calendar file

ADV - Sunday - 11:00-11:30 PDT

Title: Exploiting Voice Cloning in Adversarial Simulation
When: Sunday, Aug 11, 11:00 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

We live in an era where voice verification is increasingly adopted in security protocols. The potential for abuse through voice cloning technology presents a significant and growing threat to cybersecurity. This talk dives into the alarming capabilities of deep learning to create highly convincing voice clones. Using my own voice as a case study, I will demonstrate a recorded simulation where the cloned voice successfully bypasses several major institutions' voice verification systems. This presentation will outline the tools and techniques leveraged for voice cloning, discuss the pressing risks involved, and explore strategic countermeasures for red teams. The aim is to equip offensive security researchers with a nuanced understanding of voice cloning technology, emphasizing its implications for threat emulation and defensive strategy formulation. Attendees will gain insight into adversary tactics using publicly available voice samples for simulating voice-based attacks, providing a clear perspective on preparing defenses against such AI-driven threats.

SpeakerBio: Mark Foudy, Founder at NeurodiverseHackers.com

I am a cybersecurity professional and researcher with a robust academic background in computer science and cybersecurity from graduate school. As the head of the Hack the Box Boston Meetup and DEFCON 508, I lead efforts to cultivate a strong community of cybersecurity enthusiasts in Massachusetts. In addition to my community leadership roles, I founded and currently manage NeurodiverseHackers.com. This platform is dedicated to supporting cybersecurity practitioners in navigating their careers while managing neurodiversity and mental health challenges. Neurodiverse Hackers emphasizes inclusivity and resilience in the fast-evolving security landscape.

Return to Index - Add to Google - ics Calendar file

Title: Exploration of Cellular Based IoT Technology
When: Friday, Aug 9, 14:30 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

As cellular technologies continue to become more integrated into IoT devices, there has been a noticeable lag in comprehending potential security implications associated with cellular hardware technologies. Furthermore, the development of effective hardware testing methodologies has also fallen behind. Given the highly regulated nature of cellular communication and the prevalent use of encryption, it is imperative for security researchers to deepen their understanding of circuit design and the integration of cellular modems into IoT devices. In this presentation, I will introduce a wide-ranging testing and analysis methodology aimed at enhancing our understanding and evaluation of the security of IoT devices that currently rely on cellular communications. This methodology will encompass an examination of various cellular modem modules in use, their integration into circuit design, and hardware hacking techniques for interacting with communication circuits to control cellular modules, all for the purpose of security testing and analysis.

Speakers: Carlota Bindner,Deral Heiland

SpeakerBio: Carlota Bindner, Lead Product Security Researcher at Thermo Fisher Scientific

Carlota Bindner is a security professional with over six years of experience and has worked in penetration testing, incident response, and advisory services. In her current role as Lead Product Security Researcher at Thermo Fisher Scientific, she performs penetration tests against IoT and embedded devices, mobile apps, web applications, and thick clients, with a specialized focus on healthcare and scientific technologies. She has previously presented at RSAC and created hands-on IoT hacking labs for conferences, including RSAC and the DEF CON. Outside of work, she enjoys investigating the security of IoT and embedded systems and has recently become a member of the RF Village staff.

SpeakerBio: Deral Heiland, Principal Security Researcher (IoT) at Rapid7

Deral Heiland CISSP, serves as a Principal Security Researcher (IoT) for Rapid7. Deral has over 25 years of experience in the Information Technology field and has held multiple positions including: Senior Network Analyst, Network Administrator, Database Manager, Financial Systems Manager and Senior Information Security Analyst. Over the last 15+ years Deral's career has focused on security research, security assessments, penetration testing, and consulting for corporations and government agencies. Deral also has conducted security research on numerous technical subjects, releasing white papers, Blogs, security advisories, and has presented the information at numerous national and international security conferences including Blackhat, Defcon, Shmoocon, DerbyCon, RSAC, Hack in Paris. Deral has been interviewed by and quoted by multiple media outlets and publications including ABC World News Tonight, Cheddar TV, BBC, Consumer Reports, MIT Technical Review, SC Magazine, Dark Reading, Threat Post and Infosecurity Magazine.

Return to Index - Add to Google - ics Calendar file

BICV - Sunday - 12:30-12:59 PDT

Title: Exploring Bias in AI-Assisted News
When: Sunday, Aug 11, 12:30 - 12:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

The presentation aims to discuss the existing biases in AI-assisted news reporting. It explores how AI has been integrated into news media over the years and the implications of its use, particularly in terms of misinformation and disinformation. The goal is to spark a discussion on the role of AI in news propagation and its impact on public perception and truth. Starting with a historical overview, this presentation highlights how AI has been used by outlets like Narrative Science, the Associated Press, and the Washington Post to automate news content. The talk emphasizes the distinction between misinformation and disinformation and discusses how AI can amplify existing biases if trained on biased data. The presentation also covers the shift in news consumption towards digital platforms, the rapid spread of misinformation, and the importance of diverse media sources to prevent echo chambers.

SpeakerBio: Sydney Johns, Phd Student & Artificial Intelligence Researcher at Johns Hopkins Human Language Technology Center of Excellence

Sydney Johns is an Artificial Intelligence Researcher at the Johns Hopkins Human Language Technology Center of Excellence. She was previously a Computer Engineer in the Army C5ISR Research and Technology Integration Directorate and has worked for the JHU Applied Physics Laboratory and Northrop Grumman.

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 13:00-13:59 PDT

Title: Exploring the Cosmos: Hackable Innovations at the Allen Telescope Array
When: Saturday, Aug 10, 13:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

The Allen Telescope Array is a radio interferometer array located in Northern California. Each of the 42 antennas is 6 meters in diameter and is distributed randomly over an area of 350 meters. Each dish is sensitive to an ultra-wideband frequency range from 200 MHz to 12 GHz. While in operation, each dish can produce 1.5 GHz of bandwidth for each polarization adding up to 1.3 Tbps of data to be processed in real-time.

Although it's scale, the Allen Telescope Array acts like a gigantic Software Defined Radio. The system design gives us the ability to try new concepts not ever tried with great flexibility. This talk will go deep into how the telescope operates from the antenna's cryogenically cooled feeds to the state-of-the-art GPU-accelerated digital signal processing pipeline deployed at our on-site data center. All of this while giving special focus to little details that make it special and hackable.

SpeakerBio: Luigi Cruz

Luigi Cruz is a computer engineer working as a staff engineer at the SETI Institute. He created the CUDA-accelerated digital signal processing backend called BLADE currently in use at the Allen Telescope Array (ATA) and Very Large Array (VLA) for beam forming and high-spectral resolution observations. Luigi is also the maintainer of multiple open-source projects like the PiSDR, an SDR-specialized Raspberry Pi image, CyberEther, a heterogenous accelerated signal visualization library, and Radio Core, a Python library for demodulating SDR signals using the GPU with the help of CuPy.

Return to Index - Add to Google - ics Calendar file

Title: Exposing Coordinated Attacks Hiding in the Sheer Noise of False Positives and Lone Incidents: A Data Science Correlation and Contextualization Journey of Logs, Events, and Alerts

When: Saturday, Aug 10, 17:00 - 17:59 PDT

Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

In the complex landscape of modern cybersecurity, identifying coordinated attacks within massive volumes of security data is a formidable challenge. Security professionals often grapple with distinguishing these attacks from numerous false positives and isolated incidents. This talk will illuminate how data science can be harnessed to transform tons of heterogeneous events, logs, and alerts into a bunch of clusters, a few kill chains, and fewer actionable insights, with open-source models, and security knowledge encoding. Join us on a journey to enhance security operations efficacy and efficiency! No data science expertise is required!

Speakers:Ezz Tahoun,Lynn Hamida

SpeakerBio: Ezz Tahoun

Ezz Tahoun, a distinguished cyber-security data scientist, who won AI & innovation awards at Yale, Princeton and Northwestern. He also got innovation awards from Canada's Communications Security Establishment, Microsoft US, Trustwave US, PIA US, NATO, and more. He ran data science innovation programs and projects for OrangeCyber Defense, Forescout Technologies, Royal bank of Canada, Governments, and Huawei Technologies US. He has published 20 papers, countless articles and 15 open source projects in the domain. When he was 19 years old he started his CS PhD in one of the top 5 labs in the world for cyber & AI, in the prestigious University of Waterloo, where he published numerous papers and became a reviewer for top conferences. His designations include: SANS/GIAC-Advisory-Board, aCCISO, CISM, CRISC, GCIH, GFACT, GSEC, CEH, GCP-Professional-Cloud-Architect, PMP, BENG and MMATH. He was an adjunct professor of cyber defense and warfare at Toronto's school of management.

SpeakerBio: Lynn Hamida

Lynn Hamida (CISSP, GCIH) is an expert researcher and consultant in operational risk and big data analytics with deep experience & credentials in the fields of business risk, cyber risk, temporal event knowledge graphs, graph ontologies, risk modeling, operational threat modeling, graph analytics, process digitization, business process mining, business analysis. She finished her post-graduate studies in CyberSecurity at Univ of Toronto and Univ of Ottawa, and worked on multiple research cyberdatascience projects with Univ of Windsor, WASP, Cypienta and others.

Return to Index - Add to Google - ics Calendar file

XRV - Friday - 14:00-17:59 PDT

Title: Extend reality with tabletop RPG OWASP Cornucopia. Play sessions throughout workshop times.
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

OWASP Cornucopia is a card game to assist software development teams identify security requirements in agile, conventional, and formal software development processes. It is language, platform, and technology agnostic. Having celebrated its 10th anniversary last year, Cornucopia has been refreshed including an updated full version of the game, a new Website App Edition updated with the OWASP ASVS 4.0 mapping and a Mobile App Edition with the OWASP MASVS 2.0 mapping for mobile development.

SpeakerBio: Stryker, Head of Security Communications and Planning at Adversary Pursuit Group (APG)

Stryker is the Head of Security Communications and Planning for the Adversary Pursuit Group (APG), where she translates technical research and qualitative intelligence into the "so what?" and "what now?" solutions that keep more people safe and secure. Stryker's 2023 original cybersecurity research series "Press Reset" won multiple industry awards, including best use of original research and best data insights. You can find her on LinkedIn, Mastodon, or in the Lonely Hackers Club (LHC) Telegram chat, where she once (in)famously ranted about how commercial gun safes do not make for secure off-site data storage options. Stryker lives in the Baltimore-DC area, renovating a townhouse with her ancient beagle-hound mix and growing parsley for swallowtail butterfly caterpillars.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 12:00-13:45 PDT

Title: FACTION
When: Saturday, Aug 10, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W308 - Map

Description:

FACTION is an all-encompassing solution for streamlined security assessment workflows and enhancing collaboration within your teams. In addition, It's fully open source and extendable so it can integrate within diverse environments. FACTION's key benefits are that it cuts reporting time down to more than half for manual pen-tests, keeps tabs on all outstanding vulnerabilities with custom alerts based on your SLAs, becomes the hub of shared information for your assessments enabling other teammates to replay attacks you share, facilitates large scale assessment scheduling that typically becomes hard to manage when your teams are doing more than 100 assessments a year, and is fully extendable with REST APIs and FACTION Extensions.

SpeakerBio: Josh Summitt, Founder at Faction Security

With over 18 years of experience in application security, Josh has played diverse roles—from being a penetration tester and reverse engineer to serving as a full-stack developer and CTO of a cybersecurity startup. He founded Faction Security, an organization committed to hosting open-source tools with the goal of supporting security teams by providing resources that enhance collaboration and efficiency. In addition to making open-source security tools, Josh builds custom modular synths and generally enjoys making strange and unusual noise-making devices.

Return to Index - Add to Google - ics Calendar file

CPV - Sunday - 10:30-11:30 PDT

Title: Famous and Not-So-Famous Unsolved Codes
When: Sunday, Aug 11, 10:30 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

There are many famous codes and ciphers still waiting to be solved, such as the encrypted Voynich manuscript and Edward Elgar's Dorabella cipher. All hold a special fascination. In this talk, prepare to be entertained and informed by Elonka Dunin and Klaus Schmeh, as we briefly discuss the encryption on Kryptos, the mysterious sculpture at the center of CIA Headquarters; NKrypt, an encrypted sculpture in Australia; an encrypted engraving on an early 20th century German silver cigarette case; details about the message attached to the leg of a WWII carrier pigeon that was found in an English chimney; an encrypted postcard by the owner of UK's Luton soccer team; and the intriguing encrypted messages created by the mysterious Henry Debosnys while awaiting his murder trial in New York in the late 1800s.

Speakers: Elonka Dunin,Klaus Schmeh

SpeakerBio: Elonka Dunin, Crypto Expert

Elonka Dunin is a crypto expert and co-leader of a group that is working to crack the final cipher on the Kryptos sculpture at CIA Headquarters. She maintains a website of the World's most famous unsolved codes, and bestselling author Dan Brown named his character "Nola Kaye", a scrambled form of "Elonka", in his novel The Lost Symbol, after her.

Elonka was a member of the Board of Directors for the National Cryptologic Museum Foundation, and General Manager and Executive Producer at Simutronics, making award-winning online and mobile games.

In 2006, Elonka published The Mammoth Book of Secret Codes and Cryptograms, and with Klaus she co-wrote the book Codebreaking: A Practical Guide, with editions in 2020 and 2023.

SpeakerBio: Klaus Schmeh, Crypto Expert at Eviden

Klaus Schmeh has written 15 books (mostly in German) about cryptography, as well as over 250 articles, 25 scientific papers, and 1500 blog posts. Klaus's main fields of interest are codebreaking and the history of encryption.

Klaus is a popular speaker, known for his entertaining presentation style involving self-drawn cartoons, self-composed songs, and Lego models. He has lectured at hundreds of conferences, including the NSA Crypto History Symposium, DEF CON, and the RSA Conference.

In his day job, Klaus works as a crypto expert for the global IT security company Eviden.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 14:00-15:45 PDT

Title: Farming Ndays with GreyNoise
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W308 - Map

Description:

Gnarly vulnerabilities in devices and services that typically face the internet are being disclosed every week. You can use GreyNoise's new free community analysis platform to deploy honeypot sensors, collect PCAPs of in-the-wild exploitation of software vulnerabilities, discover the source IPs of mass scanners, botnets, and compromised devices, and compare attacks across networks. In this presentation we're demonstrating GreyNoise' new sensor deployment, SQL explorer, and rules engine.

SpeakerBio: Andrew Morris
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 18:30-19:30 PDT

Title: Feet Feud (Hacker Family Feud)
When: Saturday, Aug 10, 18:30 - 19:30 PDT
Where: LVCC West/Floor 1/Hall 1/Tracks 1-2 - Map

Description:

Feet Feud (Hacker Family Feud) is a Cybersecurity-themed Family Feud style game arranged by members of the OnlyFeet CTF team and hosted by Toeb3rius (aka Tib3rius). Both survey questions and their answers are crowd-sourced from the Cybersecurity community. Two teams (Left Foot and Right Foot) captained by members of OnlyFeet and comprised of audience members go head to head, trying to figure out the top answers to the survey questions.

Attendees can either watch the game or volunteer to play on one of the two teams. Audience participation is also encouraged if either of the two teams fails to get every answer of a survey question.

Ultimately Feet Feud is about having a laugh, watching people in the industry attempt to figure out what randomly surveyed people from the Cybersecurity community put as answers to a number of security / tech related questions.

Return to Index - Add to Google - ics Calendar file

Title: FIDO2 in the Quantum Realm
When: Sunday, Aug 11, 11:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Due to its wide usage, the FIDO2 protocol – also known as Passkeys – is a key example (pun intended) of a protocol that urgently needs to be migrated to post-quantum cryptographic algorithms (PQ or PQC) to be secure against the looming quantum threat. In this presentation we explain our work over the last two years towards maintaining secure passwordless authentication in the quantum era.

We discuss: is FIDO2 ‘quantum-ready’? Which of the used cryptographic algorithms need to be replaced and with what? What is the (quantum) threat model? And do we ‘just’ need quantum-secure instead of classical algorithms or should we instead use a combination of classical and PQ (a.k.a. hybrid) algorithms? Can the PQ migration be backwards compatible? If yes, would this introduce the possibility of down-grading attacks? And last but not least, is PQ FIDO2 feasible on current hardware?

After discussing these, we present the first end-to-end post-quantum secure implementation of the FIDO2 protocol which we have recently open-sourced and benchmarked. The aim of our E2E OSS is to provide a complete implementation that allows PQ registration and authentication in all protocol operations, to enable developers to experiment and test the viability of PQ cryptography in current hardware devices providing FIDO2 authentication.

Speakers: Nina Bindel,James Howe

SpeakerBio: Nina Bindel

Nina is a staff researcher at SandboxAQ specialized in quantum-secure algorithms and protocols, including how to ensure a smooth PQ migration of the latter. Her research has recently been focused on the FIDO2 protocol both from a theoretical as well as from a more practical aspect. Her list of publications, presentations, blog posts and a stop-motion video about batch signatures can be found at ninabindel.de.

SpeakerBio: James Howe

James is a Staff Research Scientist in the Quantum Security Group’s PQC Team. He works on the research and development of post-quantum cryptography and addresses issues in integrating PQC into the real-world. He is a co-author of the SDitH signature scheme candidate which is a part of the NIST PQC process for additional signature schemes. His research interests range from optimizing designs in software and hardware, side-channel analysis and countermeasures, protocol design, and more.

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 12:30-12:59 PDT

Title: Finding 0days in Vilo Home Routers
When: Sunday, Aug 11, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

From January to May 2024, a team of student researchers at Brigham Young University looked for 0days in a consumer-grade home router made by Vilo Living. By April 2024, they had found 9 zero days, 6 of which were critical. This presentation covers the process they went through from initial reconnaissance to hardware hacking to finding buffer overflows to reporting the bugs to the organization. Outline: Initial recon - OSINT on the company, previous vulnerabilities released (none), and black-box interactions with network services on the LAN Hardware hacking - identifying chips on the board, connecting to the UART interface, deciphering boot up info, dumping the flash memory (didn't work), and observing reads/writes by the CPU to flash memory to obtain the firmware Cloud enumeration - discovering the AWS S3 buckets and IoT infrastructure, tracing cloud interactions (authenticating to the router remotely, retrieving MQTT certificates, etc.) Firmware enumeration - kernel + libc version, arch, how to emulate binaries on an x86 machine, compiling code to run on the router, what binary does what, etc. Vulnerability discovery - finishing reversing custom TCP protocol for mobile app->router interactions, searching for stack overflows, lack of authentication, command injection (and accidentally bricking 3 routers), info leaks, reviewing the 9 vulnerabilities we discovered, weaponizing and chaining some of the vulnerabilities, etc. Vendor disclosure - difficulty contacting the vendor in May 2024 with vulnerability details (they were almost dead), how the disclosure process went, filing for CVEs in June, publishing vuln details in August Conclusion - how stupid easy it is to hack IoT devices, how IoT vendors treat security issues, where future research can focus

Speakers: Ava Petersen,Justin Mott

SpeakerBio: Ava Petersen, Student at Brigham Young University (BYU)

I'm Ava Petersen, a student at Brigham Young University pursuing an undergraduate degree in cybersecurity. I am extremely passionate about my field of study, and I love the fast-paced and creative aspect of the field which keeps me on my feet and encourages thinking outside the box to solve (or find) problems. Whether through my competitions, research, or work, I am always being challenged in new and exciting ways. You'll find me everywhere in the cybersecurity competition space under the handle "deltabluejay" and on the BYU Cyberia team.

SpeakerBio: Justin Mott, Grad Student at Brigham Young University (BYU)

Justin Mott is a grad student at BYU researching IoT security and adversary emulation. He graduated with a Bachelor's in Cybersecurity at BYU in 2023. His hobbies include CTFs, TCGs and spending time with his family.

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 12:15-12:40 PDT

Title: Finding Holes in Conditional Access Policies
When: Saturday, Aug 10, 12:15 - 12:40 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Microsoft Entra Conditional Access sits at the forefront of organization's security boundaries. The ever-changing climate of conditional access continues to give administrators more and more security controls. The tradeoff of which is increased complexity when attempting to balance security and productivity. The more policies deployed in a tenant, the greater the chance for misconfigurations that create opportunities for exploitation. Whether you're a cloud administrator, security consultant, or adversary, the goal remains the same: to find the holes in conditional access.

This talk discusses lessons learned from real-life engagements and identifies multiple strategies for evaluating conditional access. Topics and tooling are explored that view conditional access from several different angles. First, understanding PowerShell and Graph API is vital when combing through policies, finding gaps in user, group, role, location, application, or device configuration. Second, simulation of logon criteria and reporting on authentication events helps to understand where policies fall short. Finally, creating a visual representation of each policy is helpful to better see policy details or build executive reports. Each of these provides an important piece of the puzzle when attempting to identify methods to bypass security controls. Audience members should expect to leave with an arsenal of new tools and techniques to continuously monitor conditional access for risk.

SpeakerBio: Brandon Colley, Senior Security Consultant at Trimarc

Brandon Colley has over fifteen years of experience administering and securing Active Directory (AD) and Windows environments. Brandon is a Senior Security Consultant for Trimarc specializing in providing reality-based AD and Entra ID security assessments. He served as a systems administrator for multiple organizations before shifting career focus to information security. He has published multiple articles through Quest, Practical 365 and Trimarc Hub. Brandon enjoys speaking engagements and has previously presented at BsidesKC, Hackers Teaching Hackers, and PancakesCon. He co-hosts a weekly podcast, interviewing infosec professionals and has appeared on multiple broadcasts, including the Phillip Wylie Show. Brandon delivers material in a humorous, yet effective manner with a focus on content built for a Blue Team through a Red lens.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 15:30-15:59 PDT

Title: Fine Grained Authorisation with Relationship-Based Access Control
When: Friday, Aug 9, 15:30 - 15:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Who can tag me in a post? If I move this file to another folder, who now has access? If my owner breaks up with his friend, will I still get a bone?

Whether you're a human, or a dog, let's face it, authorisation is hard. Role-based access control is a great starting point but hard to scale. Attribute-based access control scales better, but neither are much good at answering more complex conditions, like whether friends-of-friends can read your posts. For such situations, we generally have to wrap this up into business logic.

This is where relationship-based access control (ReBAC) comes in, offering a nuanced approach to accessing resources without codifying that into the applications.

In this session, we'll look at how to define these relationships, experience live demos, and discover how we can deploy our own fine-grained authorisation service. Expect some tail-wagging insights and a few laughs as we explore access control from a canine's point of view.

SpeakerBio: Ben Dechrai

Ben Dechrai is a technologist with a strong focus on security and privacy. At 11 years old he wrote software to stop his parents from breaking the family PC, and now he works as a developer advocate at Sonar, helping developers avoid breaking the internet through better security and coding practices. He enjoys helping others find the joy of problem-solving and experimentation.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 12:00-12:45 PDT

Title: Fireside Chat with DNSA Anne Neuberger
When: Friday, Aug 9, 12:00 - 12:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

This fireside chat will feature an in depth conversation between DNSA Neuberger and Dark Tangent on a variety of cybersecurity and emerging technology topics such as artificial intelligence and quantum computing. DNSA Neuberger has served in a variety of senior intelligence and cybersecurity roles within the National Security Agency, including Director of NSA's cybersecurity organization and Deputy Director of NSA's intelligence operations. She has also held multiple positions at the Department of Defense and the private sector, and now leads development of the Biden Administration's policies on cybersecurity and emerging technologies from the White House. She and DT will delve into the latest and most pressing issues in these domains that concern the White House and how hackers can influence tech-related discussions to improve policy and operational outcomes.

Speakers: Anne Neuberger,Jeff "The Dark Tangent" Moss

SpeakerBio: Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Tech

As the Deputy National Security Advisor for Cyber and Emerging Tech, I serve as an advisor to the President on matters related to cybersecurity, digital innovation, and emerging technologies. I coordinate the interagency response to cyber threats and engage with allies and partners on cyber cooperation. With over 25 years of experience in the government and private sector, I try to bring a unique perspective and experience to this work, which is primarily around advancing US national security interests, enhancing cyber resilience, and fostering innovation and collaboration between the private and public sectors.

Prior to joining the White House, I led the establishment of the NSA's Cybersecurity Directorate, bringing together thousands of intelligence analysts, cybersecurity professionals, cryptographers, researchers, and technologists. I previously led NSA's global intelligence operations, and served as a White House Fellow. I care deeply about public service, inspired by the gifts this country has provided my family and so many other refugee and immigrant families.

SpeakerBio: Jeff "The Dark Tangent" Moss, DEF CON Communications
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 13:00-13:45 PDT

Title: Fireside Chat with Jay Healey and National Cyber Director Harry Coker, Jr.
When: Saturday, Aug 10, 13:00 - 13:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

The world increasingly appreciates how much we rely on space systems for our personal, economic, and national security needs. However, the nation-state cyber threat to government and commercial systems continues to grow at a time when the current landscape of cybersecurity policies and frameworks aren't readily applicable for space systems.

In this fireside chat, ONCD will have the opportunity to introduce our 2nd National Cyber Director to the research community and discuss some of his priorities, such as space cybersecurity. We will discuss how the White House has been working to tackle hard problems and challenges. In the instance of space cybersecurity, ONCD has been collaborating with federal space operators and the space industry to develop policy solutions, including by answering a tasking from the Vice President to develop minimum cybersecurity requirements for U.S. space systems.

Speakers: Harry Coker Jr.,Jay Healey

SpeakerBio: Harry Coker Jr., National Cyber Director at White House Office of the National Cyber Director (ONCD)

Harry Coker, Jr. was confirmed by the Senate on December 12, 2023 as the second National Cyber Director in the White House Office of the National Cyber Director. Director Coker is a retired Central Intelligence Agency (CIA) senior executive and career Naval Officer, is a graduate of the US Naval Academy, the Naval Postgraduate School, and Georgetown University Law Center.

Previously, Coker served as Executive Director of the National Security Agency (NSACoker's service to the Nation and NSA was recognized with the awarding of the National Intelligence Distinguished Service Medal, the NSA Director's Distinguished Service Medal, and the IC EEOD Outstanding Leadership Award.

During the first seventeen years of his service with the CIA, Coker was assigned to leadership positions in the Directorate of Digital Innovation; the Directorate of Science & Technology; and the Director's Area. Key assignments included service as Director of the Open Source Enterprise, which is responsible for leveraging publicly available information; and as Deputy Director of CIA's Office of Public Affairs. Coker's leadership and contributions earned him the Presidential Rank Award and CIA's prestigious Don Cryer Award for Diversity & Inclusion.

SpeakerBio: Jay Healey
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Firmware Extraction and Analysis
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

In this interactive exercise, you'll learn how to talk to chips on a board via SPI, extract a firmware image, and analyze it to find vulnerabilities. Take your hardware hacking skills to the next level

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Firmware Extraction and Analysis
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

In this interactive exercise, you'll learn how to talk to chips on a board via SPI, extract a firmware image, and analyze it to find vulnerabilities. Take your hardware hacking skills to the next level

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Firmware Extraction and Analysis
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

In this interactive exercise, you'll learn how to talk to chips on a board via SPI, extract a firmware image, and analyze it to find vulnerabilities. Take your hardware hacking skills to the next level

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 11:00-11:59 PDT

Title: First Time TSX Hacking Challenge
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

Never hacked into anything before? Join us at the Voting Village to learn how to hack into a voting machine yourself! No hacking skills required.

SpeakerBio: Tailor Tolliver
No BIO available

Return to Index - Add to Google - ics Calendar file

PSV - Sunday - 11:30-11:59 PDT

Title: Fitness of Physical Red Teamers
When: Sunday, Aug 11, 11:30 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Cybersecurity red teams have myriad ways of practicing their skills - from CTFs to certifications - but how do you train for physical red teaming? This talk will focus on leveling up your body - add new abilities to climb, sneak, jump, and become an unstoppable ninja while performing physical penetration tests. We'll talk about which abilities you need, and how we train ourselves (and our staff) for performing at our peak for physical engagements. This will be complemented by plenty of war stories and lessons learned in the field for what abilities are most worth leveling up in, and comparisons between red teaming before and after our weight loss. We'll then discuss different exercises and habits that the audience can start doing as soon as in your hotel room to improve your lives and your ability to break into buildings!

Speakers: Billy Graydon,Lucas Rooyakkers

SpeakerBio: Billy Graydon, Principal at GGR Security

Bill Graydon is a principal at GGR Security, where he hacks everything from locks and alarms to critical infrastructure; this has given him some very fine-tuned skills for breaking stuff. He's passionate about advancing the security field through research, teaching numerous courses, giving talks, and running the Physical Security Village at various cons. He's received various degrees in computer engineering, security, and forensics and comes from a broad background of work experience in physical and cyber security, anti-money laundering, and infectious disease detection.

SpeakerBio: Lucas Rooyakkers, Red Teamer at GGR Security

Lucas currently researches covert communications at Royal Military College, and is a red teamer at GGR Security. Formerly a software engineer for a satellite internet company (not Elon's) and a signaller in the military. Lucas has written code for several Low Earth Orbit satellites whizzing above your head in space, and for OpenSource projects. When not procrastinating thesis writing, he can often be found with an SDR trying to bypass some security system or other. Lucas also speaks Esperanto.

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 10:00-12:59 PDT

Title: Fix the Flag Wargame
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV CTF - Map

Description:

AppSec Village is proud to present our DEF CON Contest in partnership with SecDim.

Unlike a typical CTF, this contest rewards the players who fix security vulnerabilities. You can choose between secure coding challenges or competing against other players in an Attack & Defence AppSec challenge, where you need to secure your app before being given a chance to hack other players' apps .

You can also develop your own AppSec challenge by following challenge contribution guidelines. All approved challenges will be hosted during AppSec Village @ DEF CON.

There are two categories of winners: - The player with the highest total points by the end of the event (August 11 at 12:00 PM PDT) - The best-contributed challenge submission

The Award Ceremony will be held at 12:45 PM PDT in the AppSec Village on August 11.

SpeakerBio: Harley Wilson

Harley Wilson is a software engineer (intern) at SecDim, a secure coding wargame platform. With a background as a Police Officer for nine years, Harley is now channelling his expertise into the field of software development. He is pursuing a Bachelor of Computing (Software Engineering) at Curtin University, with an anticipated graduation in 2024.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 10:00-17:30 PDT

Title: Fix the Flag Wargame
When: Friday, Aug 9, 10:00 - 17:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV CTF - Map

Description:

AppSec Village is proud to present our DEF CON Contest in partnership with SecDim.

Unlike a typical CTF, this contest rewards the players who fix security vulnerabilities. You can choose between secure coding challenges or competing against other players in an Attack & Defence AppSec challenge, where you need to secure your app before being given a chance to hack other players' apps .

You can also develop your own AppSec challenge by following challenge contribution guidelines. All approved challenges will be hosted during AppSec Village @ DEF CON.

There are two categories of winners: - The player with the highest total points by the end of the event (August 11 at 12:00 PM PDT) - The best-contributed challenge submission

The Award Ceremony will be held at 12:45 PM PDT in the AppSec Village on August 11.

SpeakerBio: Harley Wilson

Harley Wilson is a software engineer (intern) at SecDim, a secure coding wargame platform. With a background as a Police Officer for nine years, Harley is now channelling his expertise into the field of software development. He is pursuing a Bachelor of Computing (Software Engineering) at Curtin University, with an anticipated graduation in 2024.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 10:00-17:30 PDT

Title: Fix the Flag Wargame
When: Saturday, Aug 10, 10:00 - 17:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV CTF - Map

Description:

AppSec Village is proud to present our DEF CON Contest in partnership with SecDim.

Unlike a typical CTF, this contest rewards the players who fix security vulnerabilities. You can choose between secure coding challenges or competing against other players in an Attack & Defence AppSec challenge, where you need to secure your app before being given a chance to hack other players' apps .

You can also develop your own AppSec challenge by following challenge contribution guidelines. All approved challenges will be hosted during AppSec Village @ DEF CON.

There are two categories of winners: - The player with the highest total points by the end of the event (August 11 at 12:00 PM PDT) - The best-contributed challenge submission

The Award Ceremony will be held at 12:45 PM PDT in the AppSec Village on August 11.

SpeakerBio: Harley Wilson

Harley Wilson is a software engineer (intern) at SecDim, a secure coding wargame platform. With a background as a Police Officer for nine years, Harley is now channelling his expertise into the field of software development. He is pursuing a Bachelor of Computing (Software Engineering) at Curtin University, with an anticipated graduation in 2024.

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: FleetDm
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

No description provided by creator

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: FleetDm
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

No description provided by creator

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: FleetDm
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

No description provided by creator

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 12:00-12:59 PDT

Title: Flipping Locks (The Remix) - Remote Badge Cloning with the Flipper Zero and More
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:
Speakers: Langston Clement,Dan Goga

SpeakerBio: Langston Clement
No BIO available
SpeakerBio: Dan Goga
No BIO available

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 17:00-17:59 PDT

Title: Flipping Locks (The Remix) - Remote Badge Cloning with the Flipper Zero and More
When: Saturday, Aug 10, 17:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Traditional RFID badge cloning methods require you to be within 3 feet of your target. So how can you conduct a physical penetration test and clone a badge without interacting with a person? Companies have increasingly adopted a hybrid work environment, allowing employees to work remotely, which has decreased the amount of foot traffic in and out of a building at any given time. This session discusses two accessible, entry-level hardware designs you can build in a day and deploy in the field, along with the tried-and-true social engineering techniques that can increase your chances of remotely cloning an RFID badge.

Langston and Dan discuss their Red Team adventures using implant devices, a Flipper Zero and an iCopy-X. As a bonus the two will explain how to perform a stealthy HID iClass SE/SEOS downgrade and legacy attack! This presentation is supplemented with files and instructions that are available for download in order to build your own standalone gooseneck reader, wall implant and clipboard cloning devices! This is. The Remix.

Speakers: Langston Clement,Dan Goga

SpeakerBio: Langston Clement
No BIO available
SpeakerBio: Dan Goga
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 13:00-13:30 PDT

Title: Fly Catcher - How I Developed a Low-Cost Raspberry Pi Based Device for ADS-B Spoof
When: Saturday, Aug 10, 13:00 - 13:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

As a pilot and cybersecurity researcher, I am very interested of the nexus between aviation and security. To explore this interest, I developed a device called Fly Catcher - a device that detects for aircraft spoofing by monitoring for malicious ADS-B signals in the 1090MHz frequency. The device consists of a 1090 MHz antenna, a Flight Aware RTL SDR, a custom 3D printed case, a portable battery charger, and a MicroUSB cable.

The device receives ADS-B information from the antenna and the software-defined radio, which is then passed into a Convolutional Neural Network written with Python to detect whether or not the aircraft is spoofed. I trained the neural network on a dataset of valid ADS-B signals as well as a generated spoofed set of aircraft signals, to teach Fly Catcher how to detect and flag any suspicious ADS-B signals. It does this by checking for discrepancies in the signal's characteristics, such as its location, velocity, and identification.

The result outputted by the neural network is then displayed onto a radar screen allowing users to detect spoofed aircraft near them. To test the device, I brought it with me for an hour-long flight to scan for a wide variety of aircraft enroute. After the flight, the data was fed into the Neural Network to analyze any spoofed aircraft I might have encountered.

SpeakerBio: Angelina Tsuboi

Angelina Tsuboi is a pilot and an aerospace cybersecurity instructor with over a decade of development experience. In addition to being a scientific researcher for NASA, she has been involved in various CubeSat initiatives and enjoys tinkering with microcontrollers.

Return to Index - Add to Google - ics Calendar file

PLV - Sunday - 11:00-11:45 PDT

Title: Flying Blind: Navigating the Turbulent Skies of Aviation Cybersecurity Regulation
When: Sunday, Aug 11, 11:00 - 11:45 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

This combination presentation and panel discussion will surface the policy and technical challenges associated with securing civil aviation, bringing together perspectives from government, industry, and aviation cybersecurity companies.

Given the continued growth in civil aviation and impending regulation in the United States of America and Europe, this talk will describe the key technical challenges and the resulting policy challenges that should be addressed to keep civil aviation secure.

Speakers: Mike Weigand,Stuart Wagner

SpeakerBio: Mike Weigand, Entrepreneur in Residence at Squadra Ventures

Michael Weigand is a defense tech founder and aviation nerd. Previously, the co-founder and Chief Growth Officer of Shift5, a company he started to build cybersecurity tools to enhance the survivability of planes, trains, and tanks, he is now an Entrepreneur in Residence at Squadra Ventures, a venture capital firm with a strong cyber and national security focus. Michael previously served in the US Army as a founding member of the Army cyber branch and helped stand up the first expeditionary and capability development units. Michael's life-long passion for aviation and hacking eventually led him into the fascinating world of domestic and international policy, regulation, and standards development, where he advocates for safer operational technology practices.

SpeakerBio: Stuart Wagner, Former Chief Digital Transformation Officer at Department of the Air Force

Stuart Wagner, former Chief Digital Transformation Officer for the Department of the Air Force, led significant policy-driven innovations from 2021-2024, advancing digital transformation across the U.S. Air Force and U.S. Space Force. He orchestrated BRAVO, the largest DoD hackathon series, producing over 200 software and hardware prototypes to support global warfighters. Wagner's policy expertise includes telemetry, data unification, NLP, and security classification. His career highlights include building and managing a 50+ engineer team at the DoD to develop Advana, an analytics platform, and initiating Gamechanger, an open-source NLP and search platform. Holding degrees from the University of Michigan, the London School of Economics, and the University of Pennsylvania, Wagner is also an active angel investor and serves on a charitable foundation board.

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 17:30-17:59 PDT

Title: Fool us Once, fool us twice... Hacking Norwegian Banks
When: Friday, Aug 9, 17:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

In 2021 we could get access to all personal bank accounts at the largest bank in Norway by using a single page paper form sent by snailmail. In addition to stealing all their money, we could also see all account transactions for the last 10 years, with details. In 2024 we have done the same thing to another bank. Why didn't the banks learn the first time? In this talk we'll explain what we did, lessons learned and why paper ID still is relevant and important to us all.

Speakers:Cecilie Wian,Per Thorsheim

SpeakerBio: Cecilie Wian

Cecilie works as a consultant within security, privacy & AI technologies. She is a recognized expert in software testing with a specialization in abusability testing. With over 10 years of experience in the IT industry, Cecilie has developed into an authority in identifying and evaluating potential abuse scenarios and security vulnerabilities in various software products.

SpeakerBio: Per Thorsheim, Founder & Organizer at PasswordsCon

Per is the founder & organizer of PasswordsCon. He revealed the Linkedin breach in 2012 & got heavily involved in the Ashley Madison breach in 2015. He is featured alongside Brian Krebs & Troy Hunt in the 3-part documentary "The Ashley Madison Affair" on Hulu.

Return to Index - Add to Google - ics Calendar file

Title: Forgetting the Fundamentals? Data Communications: Physical and Logical Explanation
When: Sunday, Aug 11, 13:30 - 13:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

Many problems in our networks are simple problems that boil down to forgotten fundamentals. Kevin reviews the communication models and demonstrates a simple password capture.

SpeakerBio: Kevin Manna

Kevin is a Professor Emeritus from Northampton Community College in Bethlehem, PA. He holds a CISSP, CCNA, Cisco CyberOps Certification and is a certified Cisco Networking Academy Instructor. He is skilled in Business Planning, Cisco Routing and Switching, Advanced Routing Technologies, International Business, Business Process Improvement, Network Design, Network and Business Consulting, and System Security and Administration. He is an educational professional with a Master of Business Administration (MBA) focused on Finance and International Economics from LaSalle University. He was the Primary Investigator for the Wall Street West Dept. of Labor grant at NCC. He has held workshops on topics including basic networking, wireless fundamentals, information security, time management, and leadership development.

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 11:30-12:30 PDT

Title: Formidable Adversaries: Responding to Breaches, Ransomware, and State-Sponsored Threat Actors
When: Friday, Aug 9, 11:30 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

For the past few years, we have had multiple instances of sophisticated cyber attacks ranging from ransomware attacks to attacks propagated by state sponsored threat actors; targeting elections, organizations, critical infrastructure etc. Organizations have had to step up and compensate with additional security controls and resources. We are living in a phase where even the most secure organizations are not immune to targeted cyber threats, the landscape of cyber security is in the state of constant evolution, with everybody playing to catch up.

This panel has been structured to delve into the complex and evolving nature of cyber adversaries. Beginning with an overview of recent cyber-attacks, breaches, and targeted ransomware incidents. We will also examine the rising wave of state sponsored threat actors, while focusing on their sophisticated adversary tactics, techniques and procedures.

This panel will focus on why organizations with even the most advanced cyber defense tooling and more than capable resources are still affected by breaches and threat actors. Our panel of experts will discuss the reasons behind these incidents and provide Insights into effective response and contentment strategies. Conversation will explore the critical components of how efficiently respond to threats, contain, and remediate them.

Additionally, the panel will also touch upon how threat intel assisted adversarial attack simulation, offensive cyber security operations could be used as proactive measures in enhancing an organization’s defense posture, offering valuable insights into the mindset and methodologies of potential attackers.

Speakers: Abhijith “Abx” B R,Adam "_whatshisface" Pennington,Ken Kato,Nikhil Mittal,Stryker

SpeakerBio: Abhijith “Abx” B R

Abhijith B R, also known by the pseudonym Abx, has more than a decade of experience in the offensive cyber security industry. Currently he is involved with multiple organizations as a consulting specialist, to help them build offensive security operations programs, improve their current security posture, assess cyber defense systems, and bridge the gap between business leadership and cyber security professionals. Abhijith’s professional exposure is stretched across multiple industries and various other sectors.

As the founder of Adversary Village, Abhijith spearheads a community driven initiative exclusively focused on adversary simulation, adversary tactics, purple teaming, threat-actor/ransomware research-emulation, and offensive security-adversary tradecraft.

SpeakerBio: Adam "_whatshisface" Pennington, Lead, ATT&CK at The MITRE Corporation

Adam Pennington leads ATT&CK® at The MITRE Corporation and collected much of the intelligence leveraged in creating ATT&CK's initial techniques.

Adam is a member of the core ATT&CK® team and the editor in chief for the ATT&CK® Blog. He has spent over a decade with MITRE studying and preaching the use of deception for intelligence gathering. Adam has presented and published several venues, including FIRST CTI, USENIX Security, and ACM Transactions on Information and System Security.

Before joining MITRE, Adam was a researcher at Carnegie Mellon's Parallel Data Lab and earned his B.S. and M.S degrees in computer science and electrical and computer engineering and the 2017 Alumni Service Award from Carnegie Mellon University.

SpeakerBio: Ken Kato, VP at Omni Federal

Breaking up bureaucracy since 2008, Ken Kato is a leader in large-scale digital transformation for highly regulated industries. It's his belief that success comes from changing how teams work with each other toward a common goal. Whether it's an austere data center with bare-metal servers, global-scale cloud deployments, or terrestrial networking in the far reaches of space, it always comes back to the people.

Ken's recent accomplishments include: being a founding member of USAF Kessel Run, the first federal software factory; building Black Pearl, the Navy's premiere DevSecOeps platform; and working with the White House to secure and scale critical cyber-infrastructure. But technology alone can't solve complex problems. With this in mind, Ken balances his years of experience with industry data to develop sustainable strategies for organizational growth and predict how decisions made today will be survivable in the years ahead.

SpeakerBio: Nikhil Mittal, Founder and Director at Altered Security

Nikhil Mittal is a hacker, infosec researcher, speaker and enthusiast.

His area of interest includes red teaming, Azure and active directory security, attack research, defense strategies and post exploitation research. He has 13+ years of experience in red teaming. He specializes in assessing security risks at secure environments that require novel attack vectors and "out of the box" approach. He has worked extensively on Azure, Active Directory attacks, defense and bypassing detection mechanisms. Nikhil has held trainings and boot camps for various corporate clients (in US, Europe and SE Asia), and at the world's top information security conferences. He has spoken/trained at conferences like DEF CON, BlackHat, BruCON and more. He is the founder of Altered Security a company focusing on hands-on enterprise security learning.

SpeakerBio: Stryker, Head of Security Communications and Planning at Adversary Pursuit Group (APG)

Stryker is the Head of Security Communications and Planning for the Adversary Pursuit Group (APG), where she translates technical research and qualitative intelligence into the "so what?" and "what now?" solutions that keep more people safe and secure. Stryker's 2023 original cybersecurity research series "Press Reset" won multiple industry awards, including best use of original research and best data insights. You can find her on LinkedIn, Mastodon, or in the Lonely Hackers Club (LHC) Telegram chat, where she once (in)famously ranted about how commercial gun safes do not make for secure off-site data storage options. Stryker lives in the Baltimore-DC area, renovating a townhouse with her ancient beagle-hound mix and growing parsley for swallowtail butterfly caterpillars.

Return to Index - Add to Google - ics Calendar file

SOC - Thursday - 12:00-12:59 PDT

Title: Friends of Bill W
When: Thursday, Aug 8, 12:00 - 12:59 PDT
Where: LVCC West/Floor 3/W301 - Map

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 12:00-12:59 PDT

Title: Friends of Bill W
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 3/W301 - Map

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 17:00-17:59 PDT

Title: Friends of Bill W
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 3/W301 - Map

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

Return to Index - Add to Google - ics Calendar file

SOC - Sunday - 12:00-12:59 PDT

Title: Friends of Bill W
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 3/W301 - Map

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

Return to Index - Add to Google - ics Calendar file

SOC - Thursday - 17:00-17:59 PDT

Title: Friends of Bill W
When: Thursday, Aug 8, 17:00 - 17:59 PDT
Where: LVCC West/Floor 3/W301 - Map

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 17:00-17:59 PDT

Title: Friends of Bill W
When: Saturday, Aug 10, 17:00 - 17:59 PDT
Where: LVCC West/Floor 3/W301 - Map

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 12:00-12:59 PDT

Title: Friends of Bill W
When: Saturday, Aug 10, 12:00 - 12:59 PDT
Where: LVCC West/Floor 3/W301 - Map

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 32 has you covered. Join us throughout the conference in the Friends of Bill W Community Space in room 301. Meetings will be Thursday, Friday, Saturday: 12:00-13:00, 17:00-18:00 Sunday 12:00-13:00

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 14:00-15:59 PDT

Title: Friendship Bracelet Making
When: Friday, Aug 9, 14:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-04 - Map

Description:

Make a friendship bracelet with an exclusive WISP charm.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 14:00-15:45 PDT

Title: Friendship Bracelet Making
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-04 - Map

Description:

Make a friendship bracelet with an exclusive WISP charm.

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 12:30-13:30 PDT

Title: From CTI to Creating Campaigns
When: Saturday, Aug 10, 12:30 - 13:30 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

The goals of this presentation is to get the participants comfortable with breaking down CTI, mapping those insights to MITRE, and creating a campaign that will bring value to their work. Everything is completely focused on post-exploitation TTPs, and their importance. We will not review how to integrate IoCs into the mapping of threats. Participants will walk away with a full example of the process, resources to explore later, and examples for thinking critically about test cases.

There is a strong purple style emphasis here, to help bridge knowledge gaps, and show the importance for defensive engineers to validate their security controls. This will not bring insight into utilizing the results for remediations, threat hunting, or any other engineering strategy.

Everything in this presentation is free or open-source. Any mentions of vendors (for CTI content) is solely for the purpose of using a research paper resource that is free to the public, and are not meant to advertise.

With an interactive session, participants will learn how: (not in this particular order) * To choose a threat/actor who is relevant to their organization * I will have a premade scenario and example ready for participants to follow along * Setting High-Level Goals for their campaign * Map their threat/actor to MITRE ATT&CK ** Overview of ATT&CK

- Simulation Vs Emulation * *how this impacts choosing content* * Combining multiple threats to create a campaign
- The Power of CTI: Explore completely free CTI resources * *will cover at least 4 explore already published campaign content Interactive Questions & Answers: Making content choices* Ex: Is X or Y a better test case for this situation? * *Create multiple layers in ATT&CK navigator, to build their campaign* * Add in open-source content, such as Atomic-Red-Team * Quick Demo & interactive: how to find the right Atomic Content
- Finalizing the Campaign
- Overview of manual options and using open-source tools for executing campaigns

Other High-level topics that will be presented: (not in this particular order) * Why create your own content if there is none available * *Your org is in the beginning stages of adopting this strategy, and you want to find a good place to start Demonstrate Value (KPIs) Budget: org cant onboard BAS/Simulator tools You have a BAS but the content isn't there for a specific threat OR its not comprehensive enough * Why focus on a threat actor's TTPs Remediations are focused on the type of attack, not a specific indicator * Adopting Threats for your organization Following a framework inspired by MITRE Accepting specific threats/actors as likely to target * Avoiding Technical Bias when choosing test cases* * particularly challenging for engineers who create detections, or work with EDR solutions.

- Make zero assumptions of whether or not a test case will get stopped/logged ** Most important to choose the most aligned content to your threat/actor's TTPs
- Convincing Benefits * *Detection Validation Strategies: High Level Overview(SIEM, EDR, DLP, ect) SOC/IR gets to see examples of a full attack chain for specific threat Detection engineering gets to understand logging/EDR/tool gaps* * Threat Hunting benefits from both of these insights
- List of Free Resources to dive more into these topics

Premise: * Organizations are becoming increasingly aware of the importance of understanding the TTPs of the threats/actors most likely to target them. * Many organizations cannot afford outside consultants, or the ability to maintain a dedicated internal offensive team. Or they want this style of testing, but don't know how to get started, or show leadership the value. * This talk is for any engineer or team leader who wants to bring Adversarial Emulation/Simulation to their organization to understand how they compare against an attack from a likely threat. It is also valuable for consultants who want to provide this service to their clients. * If someone is new to offensive techniques, this will be a way for them to think about how this strategy applies to their role, and embrace it as a defensive strategy.

The goals of this presentation is to get the participants comfortable with breaking down CTI, mapping those insights to MITRE, and creating a campaign that will bring value to their work. Everything is completely focused on post-exploitation TTPs, and their importance. We will not review how to integrate IoCs into the mapping of threats. Participants will walk away with a full example of the process, resources to explore later, and examples for thinking critically about test cases.

SpeakerBio: Noah Lazzaro
No BIO available

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 11:00-11:59 PDT

Title: From Easy Wins to Epic Challenges: Bounty Hunter Edition
When: Friday, Aug 9, 11:00 - 11:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Step into the mind of a bug bounty hunter as I take you on a journey through my own adventures in vulnerability hunting. In this presentation, I'll share some of the most intriguing bugs I've discovered, from the shockingly/stupidly simple to the mind-bendingly complex.

We'll start with the surprising simplicity of some bugs, but as the hunt isn't always so simple, I'll also reveal some complex bug chains that required advanced knowledge, lot of work and probably some hacker's intuition to know it was worth pushing further.

If you want to know how a coffee break gave me the opportunity to get infinite money, or how a vulnerable CAPTCHA helped me to break the encryption of a sensitive application - you're in the right place!

SpeakerBio: Daniel "Blaklis" Le Gall

Blaklis is a bug bounty hunter that started seven years ago, as a hobby. He co-founded a company that was doing, as one of the main activities, bug bounty hunting, and decided to get back to freelance again two years ago, to be free again.

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 10:00-10:50 PDT

Title: From Network to Network: Hands-On Pivoting Techniques in Internal Environments
When: Sunday, Aug 11, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

In this workshop, the basic concepts of pivoting will be introduced, and a hands-on experience will be provided in a realistic testing environment. Participants will learn to utilize effective tools and techniques to move from one network to another within an organization's infrastructure. Additionally, attendees will have the opportunity to set up their own Docker laboratory to perform pivoting practices in an emulated environment.

SpeakerBio: Francisco Canteli
No BIO available

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 11:30-12:30 PDT

Title: From Redlining to Weblining: Examining Broadband Deserts and Racial Injustice
When: Friday, Aug 9, 11:30 - 12:30 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

This talk dives deep into the historical context of redlining, segregation, and the enduring legacy of unequal access to technology, particularly focusing on its impact on Black communities. It examines the concept of broadband deserts, highlighting geographic disparities and their economic ramifications. Furthermore, the talk explores how the lack of broadband access hinders economic opportunities for Black individuals, including limited exposure to the tech field and decreased participation in tech and cyber-related activities from a young age. By shedding light on these issues, the presentation aims to foster awareness and discussion on strategies to bridge the digital divide and promote equitable access to technology in marginalized communities.

SpeakerBio: Dr. Fatou Sankare, Security Researcher & Professor

Dr. Fatou Sankare is a passionate professor and cyber engineer whose diverse interests span from hacking and sewing to advocating for digital equity in marginalized communities. With a robust background in cybersecurity and a knack for creative problem-solving, she dedicates her career to bridging the digital divide, ensuring underserved populations have equal access to technology and opportunities in the digital age. Through innovative educational initiatives and community outreach programs, Dr. Fatou strives to empower individuals by enhancing their technological literacy and fostering inclusive digital environments.

Return to Index - Add to Google - ics Calendar file

AIxCC - Sunday - 11:30-12:15 PDT

Title: From research to release: Transferring AIxCC results to open source software
When: Sunday, Aug 11, 11:30 - 12:15 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Fireside Chat on the importance of open-sourcing solutions and how AIxCC's approach can have a far-reaching, positive impact David A. Wheeler, Director of Open Source Supply Chain Security, Open Source Security Foundation (OpenSSF) Jeff Diecks, Technical Project Manager - AIxCC, Open Source Security Foundation (Open SSF) Chris Aniszczyk, CTO, Cloud Native Computing Foundation (CNCF)

Speakers: Dr. David A. Wheeler,Jeff Diecks,Chris Aniszczyk

SpeakerBio: Dr. David A. Wheeler, Director of Open Source Supply Chain Security at Open Source Security Foundation (OpenSSF)

"Dr. David A. Wheeler is an expert on open source software (OSS) and on developing secure software. His works on developing secure software include ""Secure Programming HOWTO"", the Open Source Security Foundation (OpenSSF) Secure Software Development Fundamentals Courses, and ""Fully Countering Trusting Trust through Diverse Double-Compiling (DDC)"". He also helped develop the 2009 U.S. Department of Defense (DoD) policy on OSS. Other works of his include ""Software Inspection: An Industry Best Practice"" and ""Ada 95: The Lovelace Tutorial"".

David A. Wheeler is the Director of Open Source Supply Chain Security at the Linux Foundation and teaches a graduate course in developing secure software at George Mason University (GMU). Dr. Wheeler has a PhD in Information Technology, a Master's in Computer Science, a certificate in Information Security, a certificate in Software Engineering, and a B.S. in Electronics Engineering, all from George Mason University (GMU). He is a Certified Information Systems Security Professional (CISSP) and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE)."

SpeakerBio: Jeff Diecks

Jeff Diecks has more than two decades of experience in technology and communications with a diverse background in operations, project management and executive leadership. A participant in open source since 1999, he’s delivered digital products and applications for dozens of universities, six professional sports leagues, state governments, global media companies, non-profits, and corporate clients.

Jeff spent 14 years in the digital agency space, scaling a team to more than 90 people and leading it through a successful acquisition and exits of the co-founders. Prior to agency work, he managed operations teams at Turner Broadcasting and produced the web site for Major League Soccer in its early years (when FTP’ing flat HTML files was a thing).

Jeff and his wife live in Alpharetta, GA, and are parents of a current sophomore at SCAD Atlanta.

SpeakerBio: Chris Aniszczyk, Cloud Native Computing Foundation (CNCF)

Chris Aniszczyk is an open source technologist with a passion for building a better world through open collaboration. He's currently a CTO at the Linux Foundation focused on developer experience and running the Cloud Native Computing Foundation (CNCF). Furthermore, he's a Partner at Capital Factory where he focuses on mentoring, advising and investing in open source and infrastructure focused startups. In a previous life, he created Twitter/X's open source program and led their open source efforts. He also served for many years on the Eclipse Foundation's Board of Directors representing the committer community and the Java Community Process (JCP) Executive Committee.

RTV - Sunday - 10:00-10:50 PDT

Title: From Runners to IdP Admin
When: Sunday, Aug 11, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

Do you think AWS Admin is the end game? Let's dive deeper into cloud native lateral movement and how Identity Providers has become the biggest C2 that has ever existed.

SpeakerBio: Sim Cher Boon
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 17:00-17:30 PDT

Title: From Theory to Reality: Demonstrating the Simplicity of SPARTA Techniques
When: Saturday, Aug 10, 17:00 - 17:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Demonstrating the transition from theorized space cyber attacks to practical proof of concepts. The presentation will utilize a simple yet effective attack, a man-in-the-middle attack, on the ground infrastructure to demonstrate how many SPARTA techniques and sub-techniques can be performed against a spacecraft from the ground infrastructure. By illustrating the significant impact of this simplified concept, we aim to emphasize the urgent need for enhanced cybersecurity measures throughout the entire lifecycle of space missions and break the inherit trust between the ground and spacecraft.

SpeakerBio: Randi Tinney, Engineering Specialist for the Cyber Assessments and Research Department, Cybersecurity and Advanced Platforms Subdivision (CAPS) at The Aerospace Corporation

Randi Tinney is an Engineering Specialist for the Cyber Assessments and Research Department, Cybersecurity and Advanced Platforms Subdivision (CAPS), at The Aerospace Corporation. In this role, Randi has focused on performing vulnerability research and exploit development on a number of specialized, ground and spacecraft, systems to support in-the-lab evaluation of customers' implementations, performing vulnerability assessments and penetration testing activities for multiple customers. Randi is also a member of the development team for the space-focused tactic, technique, and procedures (TTPs) framework called Space Attack Research and Tactic Analysis (SPARTA). She has participated in numerous cyber related war games, including LockedShields, for several years. At DEFCON 31, Randi was a member of the team that won the RedAlert ICS CTF and received a Black Badge.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 17:05-17:50 PDT

Title: Front line first aid: Triaging your DFIR emergency responders
When: Saturday, Aug 10, 17:05 - 17:50 PDT
Where: Virtual

Description:

Digital forensics and incident responders, as well as other essential emergency workers, often face high stress levels and risk burnout due to their demanding roles. This talk is for professionals, spouses, managers and corporations and will cover the following topics:

Self-Care, Hacking Health, maintaining Work-Life Balance, building a Support network, developing Mindfulness and Relaxation Techniques, using technology to Manage Workload, working with management to Create a Positive Work Environment.

Having built and lead successful DFIR practices that dealt with some of Canada's largest data breaches. I wish to impart what I have learnt over the years so others may protect and nurture their most sacred resource, people.

SpeakerBio: Neumann "scsideath" Lim, Manager at Odlum Brown

Neumann Lim is a manager at Odlum Brown where he leads the defense against criminals and state sponsored actors targeting the financial industry. Prior to this role, Neumann spent several years working with large enterprises and governments specializing in dig.

With more than 15 years of infosec experience, he has delivered numerous cyber risk assessments, coordinated national incident responses across multiple industries. Neumann has been invited to share his research and thought leadership at many security conferences such as Grayhat Con, DefCon BlueTeam Village, HTCIA, BSides, Toronto CISO Summit and CCTX.ital forensics and incident response investigating some of Canada's largest data breaches from 2018-2023.

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 10:00-10:45 PDT

Title: Fumbling into FedCyber
When: Saturday, Aug 10, 10:00 - 10:45 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Nikkia Henderson is a 14 year tenured federal government employee. In her current role she is a Senior Advisor at the Cybersecurity Infrastructure Security Agency (CISA). She serves a Cyber Supply Chain Risk Management (C-SCRM) Strategy and Governance Program lead, within CISA's Cybersecurity Division. Ms. Henderson is also the President of the Women in Cybersecurity Mid Atlantic Affiliate, where she serves as a "cybHERprenuer" who is passionate about helping Cybersecurity/IT professionals define their vision, mission, and federal career path. In this session, Ms. Henderson shares her journey into a federal cyber career. She will highlight her challenges as well as milestones that catapulted her to where she is today!

SpeakerBio: Nikkia Henderson, Program Operations Lead

Nikkia Henderson is a 14 year tenured federal government employee. In her current role she is a Senior Advisor at the Cybersecurity Infrastructure Security Agency (CISA). She serves a Cyber Supply Chain Risk Management (C-SCRM) Strategy and Governance Program lead, within CISA's Cybersecurity Division. Ms. Henderson is also the President of the Women in Cybersecurity Mid Atlantic Affiliate, where she serves as a "cybHERprenuer" who is passionate about helping Cybersecurity/IT professionals define their vision, mission, and federal career path. In this session, Ms. Henderson shares her journey into a federal cyber career. She will highlight her challenges as well as milestones that catapulted her to where she is today!

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 15:00-15:59 PDT

Title: FuzzLLM: A Fuzzing Framework for Discovering Jailbreak Vulnerabilities in Large Language Models
When: Saturday, Aug 10, 15:00 - 15:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Jailbreak vulnerabilities in Large Language Models (LLMs), which exploit meticulously crafted prompts to elicit content that violates service guidelines, have captured the attention of research communities. While model owners can defend against individual jailbreak prompts through safety training strategies, this relatively passive approach struggles to handle the broader category of similar jailbreaks. To tackle this issue, we introduce FuzzLLM, an automated fuzzing framework designed to proactively test and discover jailbreak vulnerabilities in LLMs. We utilize templates to capture the structural integrity of a prompt and isolate key features of a jailbreak class as constraints. By integrating different base classes into powerful combo attacks and varying the elements of constraints and prohibited questions, FuzzLLM enables efficient testing with reduced manual effort. Extensive experiments demonstrate FuzzLLM's effectiveness and comprehensiveness in vulnerability discovery across various LLMs.

SpeakerBio: Ian G. Harris, Professor of Computer Science at University of California Irvine

Ian G. Harris is Professor of Computer Science at the University of California Irvine. He received his BS degree in Computer Science from Massachusetts Institute of Technology in 1990. He received his MS and PhD degrees in Computer Science from the University of California San Diego in 1992 and 1997 respectively. He was a member of the faculty in the Electrical and Computer Engineering Department at the University of Massachusetts Amherst from 1997 until June 2003.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Game Hacking Community Activities & CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-03 - Map

Description:

Welcome to the inaugural GameHacking.GG @ DEF CON 32, where gaming and cybersecurity intersect in exciting and interactive ways. Our mission is to delve into various aspects of game security, fostering an environment of exploration, play, and learning. The DEFCON32 event is constructed to make game security accessible and playable at all skill levels.

At the Game Hacking DEF CON 32 event, participants can engage in activities ranging from modding games to exploring the intricacies of memory hacking and multiplayer cheats. In future iterations of the event we hope to expand to learning about game malware and maybe even some hardware hacks. Whether you're a beginner or an experienced hacker, we will have presentations and activities to challenge your skills.

Be part of the evolution of game security. Dive into our activities, engage with other game hackers, and explore opportunities to contribute to and support the Game Hacking Community. Let’s play, learn, exploit, and perhaps even profit.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-10:59 PDT

Title: Game Hacking Community Activities & CTF
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-03 - Map

Description:

Welcome to the inaugural GameHacking.GG @ DEF CON 32, where gaming and cybersecurity intersect in exciting and interactive ways. Our mission is to delve into various aspects of game security, fostering an environment of exploration, play, and learning. The DEFCON32 event is constructed to make game security accessible and playable at all skill levels.

At the Game Hacking DEF CON 32 event, participants can engage in activities ranging from modding games to exploring the intricacies of memory hacking and multiplayer cheats. In future iterations of the event we hope to expand to learning about game malware and maybe even some hardware hacks. Whether you're a beginner or an experienced hacker, we will have presentations and activities to challenge your skills.

Be part of the evolution of game security. Dive into our activities, engage with other game hackers, and explore opportunities to contribute to and support the Game Hacking Community. Let’s play, learn, exploit, and perhaps even profit.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Game Hacking Community Activities & CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-03 - Map

Description:

Welcome to the inaugural GameHacking.GG @ DEF CON 32, where gaming and cybersecurity intersect in exciting and interactive ways. Our mission is to delve into various aspects of game security, fostering an environment of exploration, play, and learning. The DEFCON32 event is constructed to make game security accessible and playable at all skill levels.

At the Game Hacking DEF CON 32 event, participants can engage in activities ranging from modding games to exploring the intricacies of memory hacking and multiplayer cheats. In future iterations of the event we hope to expand to learning about game malware and maybe even some hardware hacks. Whether you're a beginner or an experienced hacker, we will have presentations and activities to challenge your skills.

Be part of the evolution of game security. Dive into our activities, engage with other game hackers, and explore opportunities to contribute to and support the Game Hacking Community. Let’s play, learn, exploit, and perhaps even profit.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 12:00-12:59 PDT

Title: Game Hacking Community Closing Talk & Awards Ceremony
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-03 - Map

Description:

Return to Index - Add to Google - ics Calendar file

AIV - Saturday - 11:30-12:30 PDT

Title: garak : A Framework for Large Language Model Red Teaming
When: Saturday, Aug 10, 11:30 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Large Language Model (LLM) deployment and integration comes with a need for scalable evaluation of how these models respond to adversarial attacks. However, LLM security is a moving target: models produce unpredictable output, are constantly updated, and the potential adversary is highly diverse: anyone with access to the internet and a decent command of natural language. Further, what constitutes a weakness in one context may not be an issue in a different context; one-fits-all guardrails remain theoretical. It is time to rethink what constitutes ``LLM security'', and pursue a holistic approach to LLM security evaluation, where exploration and discovery of issues are central. To this end, this paper introduces garak (Generative AI Red-teaming and Assessment Kit), a framework which can be used to discover and identify vulnerabilities in a target LLM or dialog system. garak probes an LLM in a structured fashion to discover potential vulnerabilities. The outputs of the framework describe a target model's weaknesses, contribute to an informed discussion of what composes vulnerabilities in unique contexts, and can inform alignment and policy discussions for LLM deployment.

Speakers: Leon Derczynski,Erick Galinkin,Jeffery Martin,Subho Majumdar

SpeakerBio: Leon Derczynski, Principal Research Scientist, LLM Security at NVIDIA

Leon Derczynski is principal research scientist in LLM Security at NVIDIA and prof in natural language processing at ITU Copenhagen. He's on the OWASP LLM Top 10 core team, and consults with governments and supranational bodies. He co-wrote a paper on how LLM red teaming is like demon summoning, that you should definitely read. He's been doing NLP since 2005, deep learning since it was more than one layer, and LLM security for about two years, which is almost a lifetime in this field. Finally, Prof. Derczynski also contributes to ML Commons, and regularly appears in national and international media.

SpeakerBio: Erick Galinkin, Research Scientist at NVIDIA

Erick Galinkin is a Research Scientist at NVIDIA working on the security assessment and protection of large language models. Previously, he led the AI research team at Rapid7 and has extensive experience working in the cybersecurity space. He is an alumnus of Johns Hopkins University and holds degrees in applied mathematics and computer science. Outside of his work, Erick is a lifelong student, currently at Drexel University and is renowned for his ability to be around equestrians.

SpeakerBio: Jeffery Martin, NVIDIA
No BIO available
SpeakerBio: Subho Majumdar, vijil
No BIO available

Return to Index - Add to Google - ics Calendar file

DL - Friday - 14:00-15:45 PDT

Title: Garak
When: Friday, Aug 9, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W306 - Map

Description:

Garak, Generative AI Red-teaming and Assessment Kit, is a vulnerability scanner for large language models (LLMs) and dialogue systems. It has a host of different probes, each working on different vulnerabilities and payloads. It connects to a broad range of different LLMs. The attacks range between static tests of fixed prompts, to dynamically assembled prompts, to probes that respond to existing model behavior when working out their next move. Community contribution plays a big part of Garak already, with an active repo & over 300 members in the Discord. Garak can assess and attack anything that takes text and returns text, and is already used by many industry players in assessment of internal and external models, including NVIDIA and Microsoft as well as a range of emerging AI Security startups; it's the #1 ranked tool for LLM security on Hackernews. But we think it's mostly a lot of fun.

Speakers: Erick Galinkin,Leon Derczynski

SpeakerBio: Erick Galinkin, Research Scientist at NVIDIA

Erick Galinkin is a Research Scientist at NVIDIA working on the security assessment and protection of large language models. Previously, he led the AI research team at Rapid7 and has extensive experience working in the cybersecurity space. He is an alumnus of Johns Hopkins University and holds degrees in applied mathematics and computer science. Outside of his work, Erick is a lifelong student, currently at Drexel University and is renowned for his ability to be around equestrians.

SpeakerBio: Leon Derczynski, Principal Research Scientist, LLM Security at NVIDIA

Leon Derczynski is principal research scientist in LLM Security at NVIDIA and prof in natural language processing at ITU Copenhagen. He's on the OWASP LLM Top 10 core team, and consults with governments and supranational bodies. He co-wrote a paper on how LLM red teaming is like demon summoning, that you should definitely read. He's been doing NLP since 2005, deep learning since it was more than one layer, and LLM security for about two years, which is almost a lifetime in this field. Finally, Prof. Derczynski also contributes to ML Commons, and regularly appears in national and international media.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 12:00-13:45 PDT

Title: GC2 - The First Serverless Command & Control
When: Saturday, Aug 10, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W306 - Map

Description:

GC2 is the first serverless command and control. This project aims to demonstrate how attackers could take advantage of third-party tools (Google Sheets and Google Drive) to execute commands and exfiltrate information from a compromised system. First released in 2021, became well known in April 2023 after being mentioned in Google's Threat Horizons Report.

SpeakerBio: Lorenzo Grazian

Lorenzo Grazian has more than 6 years of experience in red teaming, penetration testing and source code review mainly in the financial and transport industries. He worked and led local and global cybersecurity projects. Besides his offensive security background, he developed several tools to support offensive security activities.

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 10:00-10:30 PDT

Title: GCPwn: A Pentester's GCP Tool
When: Saturday, Aug 10, 10:00 - 10:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

When discussing the various cloud providers within the last decade, Google Cloud Platform (GCP) is often seen as the smaller provider following AWS and Azure with regards to market share. While GCP might appear smaller than its rival cloud providers, it still is very much in use today, and with this use comes the opportunities for developing pentesting tools. As I've been learning GCP over the last year, I have been making a framework in python (much like Pacu for AWS) specifically for GCP. This includes enumeration modules for some of the core services (Cloud Storage, Cloud Functions, Cloud Compute, IAM) along with the incorporation of numerous exploit modules, many of them rooted in Rhino Security's currently public GCP exploit repository (https://github.com/RhinoSecurityLabs/GCP-IAM-Privilege-Escalation/tree/master). In addition, the framework is built such that it should be easy for a first-time GCP user or beginner to code and develop modules that focus on purely navigating individual resources and easily drop those into the framework. The overall goal is to make an up-to-date, maintained enumeration and exploit toolset for GCP pentesters/red teams/researchers alike that reduces the barrier of entry for learning GCP by allowing average users to make their own modules that easily incorporate with the overall framework.

SpeakerBio: Scott Weston

Originally from southern CA, I am currently a senior security consultant for NetSPI based out of Minneapolis, MN. My assessment experience includes web applications, AWS, GCP, and external networks. I spoke about AWS organizations at fwd:cloudsec 2023 with most of the talk summarized in the 2 part blogpost here: https://www.netspi.com/blog/technical-blog/cloud-pentesting/pivoting-clouds-aws-organizations-part-1/. I got accepted to speak at fwd:cloudsec 2024 for a new tool I've been making to pentest GCP environments (mirroring Pacu-like structure). In my spare time I like to pursue bug bounties if the opportunity arises, play videogames, assume the role of dungeon master every so often, and just hang out.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 15:00-15:45 PDT

Title: Generative AI vs Crusty NCO
When: Friday, Aug 9, 15:00 - 15:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:
SpeakerBio: Col Travis Hartman
No BIO available

Return to Index - Add to Google - ics Calendar file

AIV - Friday - 10:30-11:30 PDT

Title: Generative Red Team 2 Kickoff
When: Friday, Aug 9, 10:30 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Come ask us anything about the GRT2! There will be a short presentation about how to participate and the objectives of the event and then you can ask us anything about it and ML flaws and vulnerabilities.

Speakers: Sven Cattell,Will Pearce,Jerome Wynne,Sean McGregor,Nicole DeCario,Kent Wilson

SpeakerBio: Sven Cattell, Founder at AI Village
No BIO available
SpeakerBio: Will Pearce
No BIO available
SpeakerBio: Jerome Wynne
No BIO available
SpeakerBio: Sean McGregor
No BIO available
SpeakerBio: Nicole DeCario
No BIO available
SpeakerBio: Kent Wilson
No BIO available

Return to Index - Add to Google - ics Calendar file

AIV - Sunday - 12:00-12:59 PDT

Title: Generative Red Team 2 Readout & Acknowledgements
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

We’re going over the results of the GRT and giving out some awards for our favorite reports. We want to hear from you about how it went and what you liked.

Speakers: Sven Cattell,Will Pearce,Jerome Wynne,Sean McGregor,Nicole DeCario,Kent Wilson

SpeakerBio: Sven Cattell, Founder at AI Village
No BIO available
SpeakerBio: Will Pearce
No BIO available
SpeakerBio: Jerome Wynne
No BIO available
SpeakerBio: Sean McGregor
No BIO available
SpeakerBio: Nicole DeCario
No BIO available
SpeakerBio: Kent Wilson
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 15:00-15:45 PDT

Title: GeoINT Mastery: A pixel is worth a thousand words
When: Friday, Aug 9, 15:00 - 15:45 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

After this interactive talk, you will never see images the same way again. This enlightening session explores the dynamic realm of GEOINT (Geospatial Intelligence), a captivating subset of OSINT (Open Source Intelligence) that unlocks a wealth of hidden insights within images and videos. From identifying objects, landscapes, and aircraft to interpreting symbols, shadows, and reflections, we'll go deep into the art of imagery analysis. Learn how to decode the language of trees, signs, text and logos, and uncover the strategic implications behind seemingly mundane details using common browser tools. This talk promises to equip you with mind-blowing skills that you can easily learn as I take you through multiple demos.

SpeakerBio: Mishaal Khan
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 15:00-15:50 PDT

Title: GHOST in the Model: Generating AI-Assisted Threat Models for Efficient Offensive Security Testing
When: Friday, Aug 9, 15:00 - 15:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

Step into a cybernetic world where humanity and technology intertwine in a complex dance of evolution. Just like the cyberpunk masterpiece, we will augment our cybersecurity defenses through the fusion of artificial intelligence and human ingenuity.

In this presentation, we explore the symbiotic relationship between humans and AI, mirroring the fusion of man and machine in Ghost in the Shell. Through the lens of AI-enhanced threat modeling, we uncover how Generative Artificial Intelligence Language Models (GenAI LLMs) empower penetration testing and red teaming professionals to transcend traditional boundaries and improve security early in the design process. Additionally, they contribute to more efficient testing of completed systems and applications.

Join us as we journey through the cybernetic landscape, where attendees will learn to merge human intuition with AI intelligence to fortify solutions and improve offensive security testing. Together, we will transcend the limitations of conventional approaches and embrace the cybernetic evolution that awaits us.

SpeakerBio: Sam Cosentino
No BIO available

Return to Index - Add to Google - ics Calendar file

PLV - Saturday - 13:00-13:45 PDT

Title: Global Perspectives in Cybersecurity: Challenging Norms and Expanding Horizons
When: Saturday, Aug 10, 13:00 - 13:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

This panel aims to mobilize DEFCON's technical talent towards global good, encouraging application of their skills in a broader, impactful context. Transcending conventional cybersecurity dialogues focused primarily on the US and Europe, this discussion highlights underexplored regions and emphasizes the importance of partnerships and incorporating international developments into cybersecurity strategies. Attendees will learn from Mr. Randy Pestana on how academic institutions contribute to cybersecurity, followed by Ms. Kerry Ann Barrett on the influence of multilateral organizations, Mr. Brett DeWitt on financial sector insights that influence foreign investment, and Mr. Wouter Veenstra on the necessity of global collaboration. This session equips participants to engage more effectively in international cybersecurity efforts, highlighting the value of diverse global perspectives and strategic partnerships.

Speakers: Wouter Veenstra,Randy Pestana,Kerry-Ann Barrett,Brett DeWitt

SpeakerBio: Wouter Veenstra, GFCE

Wouter Veenstra is in the lead of GFCE Outreach and Partnerships and his key responsibilities are to identify and connect key stakeholders on Cyber Capacity Building, to interest them to join the GFCE and to connect them on cyber topics based on their wants, needs and means.

SpeakerBio: Randy Pestana, Director of Cybersecurity Polic at Florida International University's Jack D. Gordon Institute for Public Policy

Randy Pestana serves as Director of Cybersecurity Policy at Florida International University's Jack D. Gordon Institute for Public Policy. He is responsible for managing the institutes cyber-related partnerships to include U.S. government entities, multilateral organizations and numerous industry partners across the cybersecurity community.

SpeakerBio: Kerry-Ann Barrett, Cybersecurity Program Manager at Inter-American Committee Against Terrorism of the Organization of American States

Kerry-Ann Barrett is the Cybersecurity Program Manager within the Inter-American Committee Against Terrorism of the Organization of American States (OAS/CICTE). In her capacity she leads the OAS/CICTE's cybersecurity capacity building efforts to member states through the design, planning and execution of cybersecurity initiatives.

SpeakerBio: Brett DeWitt, Mastercard

Brett DeWitt drives global cybersecurity public policy strategies to enable a more secure, inclusive, and innovative digital economy. Brett represents Mastercard in international trade associations, engages in public-private partnerships, supports the development of policy solutions for governments, and coordinates external communications.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-17:59 PDT

Title: Gold Bug Challenge
When: Sunday, Aug 11, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-F - Map

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle can keep you intrigued and busy throughout DEF CON - and questioning how deep the layers of cryptography go.

The Gold Bug is an annual puzzle hunt at DEF CON, focused on cryptography. You can learn about Caesar ciphers, brush up your understanding of how Enigma machines or key exchanges work, and try to crack harder modern crypto.

The Gold Bug is accessible to all, with some simpler puzzles for warmup or beginners (even kids!), and some that will require you to dig a little deeper. Whether you want to hack on puzzles solo or with a team, join us at https://goldbug.cryptovillage.org to get started!

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Gold Bug Challenge
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-F - Map

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle can keep you intrigued and busy throughout DEF CON - and questioning how deep the layers of cryptography go.

The Gold Bug is an annual puzzle hunt at DEF CON, focused on cryptography. You can learn about Caesar ciphers, brush up your understanding of how Enigma machines or key exchanges work, and try to crack harder modern crypto.

The Gold Bug is accessible to all, with some simpler puzzles for warmup or beginners (even kids!), and some that will require you to dig a little deeper. Whether you want to hack on puzzles solo or with a team, join us at https://goldbug.cryptovillage.org to get started!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Gold Bug Challenge
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-F - Map

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle can keep you intrigued and busy throughout DEF CON - and questioning how deep the layers of cryptography go.

The Gold Bug is an annual puzzle hunt at DEF CON, focused on cryptography. You can learn about Caesar ciphers, brush up your understanding of how Enigma machines or key exchanges work, and try to crack harder modern crypto.

The Gold Bug is accessible to all, with some simpler puzzles for warmup or beginners (even kids!), and some that will require you to dig a little deeper. Whether you want to hack on puzzles solo or with a team, join us at https://goldbug.cryptovillage.org to get started!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-11:59 PDT

Title: Gold Bug Challenge
When: Friday, Aug 9, 10:00 - 11:59 PDT
Where: Virtual

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle can keep you intrigued and busy throughout DEF CON - and questioning how deep the layers of cryptography go.

The Gold Bug is an annual puzzle hunt at DEF CON, focused on cryptography. You can learn about Caesar ciphers, brush up your understanding of how Enigma machines or key exchanges work, and try to crack harder modern crypto.

The Gold Bug is accessible to all, with some simpler puzzles for warmup or beginners (even kids!), and some that will require you to dig a little deeper. Whether you want to hack on puzzles solo or with a team, join us at https://goldbug.cryptovillage.org to get started!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 14:00-14:59 PDT

Title: Gold Bug: Puzzle Panel
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Welcome to Day 2 of the Gold Bug at the 11th annual Crypto & Privacy Village! Join the Gold Bug Team for the latest updates, panel-exclusive hints, and more. This panel compliments the Gold Bug: Welcome on Day 1.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-12:59 PDT

Title: Gold Bug: Welcome
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

Welcome to the Gold Bug at the 11th annual Crypto & Privacy Village! This opening talk compliments the Gold Bug: Puzzle Panel on Day 2.

The Gold Bug Team 2024 at the Crypto & Privacy Village: 0xCryptok, tseven, llamaprincess, pleoxconfusa, Pascal-0x90, Delta_JRM, are the beloved puzzle-makers within Crypto & Privacy Village. We make a special effort to include accessible puzzles at all skill levels. It is our hope that anyone, from new puzzlers (even kids!) to seasoned puzzle hunters, can participate in and enjoy this contest.

The GoldBug team also runs Crypto & Privacy Village's Junior Cryptography at DC NextGen.

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 10:10-10:50 PDT

Title: Gone in 60 Seconds… How Azure AD/Entra ID Tenants are Compromised
When: Friday, Aug 9, 10:10 - 10:50 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

60 seconds. 1 minute.

That's all it takes for an attacker to compromise an account with access. And the account doesn't even need to have obvious privileged rights for the attacker to own the cloud environment.

Then, once they get Global Admin rights to Azure AD/Entra ID, it's game over since they have full admin rights, access to all data, and can easily pivot to control all Azure subscription services and content.

This talk walks through the most common ways that attackers compromise the Microsoft Cloud, specifically Azure AD/Entra ID and how to mitigate these attack techniques.

Join me in this journey of attacker methods involving account compromise of admin and user accounts, including interesting pairing of role rights, application permissions, and Conditional Access gaps.

So go beyond Global Administrator to better understand the Entra ID roles that really matter in the tenant and how application permissions provide attacker opportunity in most environments!

Attendees will learn both Azure AD/Entra ID attack and defense during this session.

SpeakerBio: Sean Metcalf

Sean Metcalf is founder and CTO at Trimarc (TrimarcSecurity.com), a professional services company which focuses on improving enterprise security. He is one of about 100 people in the world who holds the Microsoft Certified Master Directory Services (MCM) Active Directory certification, is a former Microsoft MVP, and has presented on Active Directory, Azure AD/Entra ID, & Microsoft Cloud attack and defense at security conferences such as Black Hat, Blue Team Con, BSides, DEF CON, DerbyCon, Troopers, & the internal Microsoft BlueHat security conference. Sean is also a co-host on the popular weekly podcast Enterprise Security Weekly streamed live every Thursday with recordings available on YouTube. You may have read some of his Active Directory & Azure AD security articles on his site, ADSecurity.org.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 21:00-01:59 PDT

Title: GOTHCON 2024
When: Friday, Aug 9, 21:00 - 01:59 PDT
Where: LVCC West/Floor 3/W322-W324, W327 - Map

Description:

Returning for their 7th year, Gothcon invites you to come dance the night away with a line-up of some of the community's best dark dance music DJ's from across the US! Dress however you would like in whatever makes you feel comfortable and happy, and all are welcome (except nazis). Follow @dcgothcon on X for current updates on lineup and other surprises we have in store.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 10:30-11:15 PDT

Title: Gotta Cache ‘em all: bending the rules of web cache exploitation
When: Saturday, Aug 10, 10:30 - 11:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

In recent years, web cache attacks have become a popular way to steal sensitive data, deface websites, and deliver exploits. We've also seen parser inconsistencies causing critical vulnerabilities like HTTP Request Smuggling. This raises the question: what happens if we attack web caches' URL-parsers?

In this session, I'll introduce two powerful new techniques that exploit RFC ambiguities to bypass the limitations of web cache deception and poisoning attacks.

First, I'll introduce Static Path Deception, a novel technique to completely compromise the confidentiality of an application. I’ll illustrate this with a case study showing how such a breach can be replicated in environments like Nginx behind Cloudflare.

Next, I'll present Cache Key Confusion, and show how to exploit URL parsing inconsistencies in major platforms, including Microsoft Azure Cloud. I’ll then show how to achieve arbitrary cache poisoning and full denial of service.

Finally, I'll reveal how to supercharge these vulnerabilities with a live demo that blends Cache Key Confusion with a “non-exploitable” open redirect to execute arbitrary JS code for complete site takeover.

Attendees will depart armed with a set of innovative techniques, along with a definitive methodology to find and exploit these and other URL or HTTP discrepancies.

Web Cache Deception Attack - Omer Gil link

This is the first time Web Cache Deception attacks were introduced and worked as a starting point for my research.

Web Cache Entanglement: Novel Pathways to Poisoning - James Kettle link

This research worked as an inspiration to develop the cache poisoning techniques. I also used this paper to outline the state of the art in web cache exploitation and create a different approach using parser discrepancies.

Cached and confused: Web cache deception in the wild - Seyed Ali Mirheidari, Sajjad Arshad, Kaan Onarlioglu, Bruno Crispo, Engin Kirda and William Robertson. link

The web cache deception techniques using delimiters for path confusion were inspired by the 2020 USENIX presentation “Cached and confused: Web cache deception in the wild”. In that presentation, they briefly describe some variations of path confusion using four encoded characters. Although the objective of their paper was to show a large-scale study of web cache deception vulnerabilities in the wild, it also introduced the use of delimiters for path confusion. In my presentation I'll expand on this concept, providing a methodology to find all the delimiters used by a URL parser and explaining how to use them in new exploitation techniques.

ChatGPT Account Takeover - Wildcard Web Cache Deception - Harel Security Research link

Also, during the time this research was being conducted, a vulnerability using a single variation of one of the techniques (Static Path Confusion) was published as a write up.

SpeakerBio: Martin Doyhenard, Security Researcher at Portswigger

Martin Doyhenard is a Security Researcher at Portswigger, known for exploiting HTTP servers and web applications. Over the past few years he has presented his findings in multiple top security conferences including BlackHat, DEFCON, RSA, EkoParty, Hack in The Box and Troopers.

His latest work includes discovering HTTP Response Smuggling techniques and exploiting SAP's Inter-Process Communication service - compromising more than 200 thousand companies in the world.He's also passionate about low level reverse engineering and testing his skills in online CTFs.

Return to Index - Add to Google - ics Calendar file

TCV - Saturday - 11:00-13:59 PDT

Title: GPON Unplugged
When: Saturday, Aug 10, 11:00 - 13:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

Join us at Telecom Village, DEFCON for an in-depth GPON workshop. We'll explore GPON technology basics, standards, capabilities, and deployment methods, while identifying vulnerabilities and advanced mitigation strategies. The workshop features a live GPON setup and performance test for hands-on experience. Ideal for telecom professionals, network engineers, cybersecurity experts, and tech enthusiasts eager to deepen their understanding of modern telecommunications.

SpeakerBio: Akib Sayyed, Founder and Director at Matrix Shell Technologies

Akib, Founder and Director of Matrix Shell Technologies, has over 12 years of experience in Telecom Security. He has served diverse telecom operators across India, Africa, and the Middle East, specializing in signaling protocols and technologies like GSM, UMTS, LTE, 5G, and VoLTE. He has led numerous penetration testing projects, disclosed a GSM vulnerability in 2012, and worked with various open-source telecom platforms. Akib has also delivered training at Black Hat and DEFCON, contributing significantly to the cybersecurity community. His education includes a Bachelor's in Engineering (CSE) and certifications in ISO 17025:2017 and 5G.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 12:30-12:59 PDT

Title: GPS spoofing: it's about time, not just position
When: Saturday, Aug 10, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Talking to pilots and operators, an important aspect of GPS spoofing and jamming is being missed from the narrative in the media. We know about position spoofing, that's a given. What doesn't appear to be getting much attention is the effect of time spoofing.

The most significant of these is an incident where time was spoofed a significant period into the future. This caused all digital certificates on board an aircraft to become invalid and caused all electronic communications to fail. As GPS clocks have protection against time being rolled backwards, but not forward, the aircraft was grounded for several weeks for systems to be reflashed and the clocks to be reset,

Coarse time spoofing could therefore ground entire fleets. We'll discuss this and potential mitigations. If time allows, we could touch on conventional RF navaids and their exposure to similar attacks.

SpeakerBio: Ken Munro, Partner and Founder at Pen Test Partners

Ken Munro is Partner and Founder of Pen Test Partners, a firm of ethical hackers. He and colleagues hold private pilot's licenses and have been interested in aviation security for many years. They also publish and blog about their research into aviation cyber security, covering topics from airborne connectivity, the potential risks of publicly available avionics component information, and even the entire attack surface of the modern airport. Ken and Pen Test Partners have also been invited to speak at various aviation industry events, and on aviation at specialist security events such as DEF CON's Aerospace Village, the Global Connected Aircraft Summit, and the Aviation ISAC Summit among others.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 12:00-12:45 PDT

Title: Grand Theft Actions: Abusing Self-Hosted GitHub Runners at Scale
When: Saturday, Aug 10, 12:00 - 12:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

GitHub Actions is quickly becoming the de facto CI/CD provider for open-source projects, startups, and enterprises. At the same time, GitHub's security model is full of insecure defaults. This makes it easy for their customers to expose themselves to critical attacks from the public internet. The end result? A systemic vulnerability class that won't go away.

During our research, we identified GitHub Actions misconfigurations at scale that would allow threat actors to backdoor major open-source projects. An example of this is our attack on PyTorch, a prominent ML framework used by companies and researchers around the world.

Through this attack, we could contribute code directly to the main branch of the PyTorch repository, upload malicious releases, backdoor other PyTorch projects, and more. These attacks began by compromising self-hosted runners, which are machines that execute jobs in a GitHub Actions workflow. From there, we leveraged misconfigurations and GitHub "features" to elevate our privileges within GitHub Actions workflows.

Our research campaign included dozens of reports, over $250,000 in bug bounties, and endless war stories. Tune in for a deep dive into the TTPs that allow turning a trivial runner compromise into a full supply chain attack.

1. link
2. link
3. link

Speakers: Adnan Khan,John Stawinski

SpeakerBio: Adnan Khan, Red Team Security Engineer

Adnan is a Red Team Security Engineer and researcher who has recently been focusing on supply chain and CI/CD attacks. He has identified, demonstrated, and reported vulnerabilities impacting GitHub repositories belonging to organizations like Microsoft, Nvidia, GitHub, Google, and more. Additionally, he has spoken at conferences such as ShmooCon 2023 and BSides SF 2023 on the topic of GitHub Actions security.

SpeakerBio: John Stawinski

John is an offensive security engineer, vulnerability researcher, and writer, specializing in Red Team operations and CICD security. John established himself as a member of the broader security community in 2023 through a series of CI/CD attacks on prominent open-source repositories. Embracing a nomadic lifestyle, John thrives on adventure sports and welcomes new experiences.

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 11:00-11:30 PDT

Title: Gridlock: The Dual-Edged Sword of EV and Solar APIs in Grid Security
When: Sunday, Aug 11, 11:00 - 11:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

In this talk, we delve deep into the increasingly interconnected world of electronic vehicles (EVs), photovoltaic (PV) solar systems, and the broader power grid infrastructure—a nexus that is becoming a fertile ground for potential large-scale cyber disruptions. As we navigate through this complex interplay of technology and infrastructure, we will uncover the critical vulnerabilities lurking within the API connections that bind these systems together. Our exploration will not only highlight these weaknesses but will also demonstrate, through real-world scenarios and potential attack vectors, how they can be exploited to launch sophisticated cyber-attacks, emphasizing the urgent need for robust security frameworks and proactive cybersecurity measures to safeguard our collective future. The advent of PV inverters and EV charging systems has been marred by the industry's "rush to market" mentality, leading to overlooked security considerations.

SpeakerBio: Vangelis Stykas, Chief Technology Officer at Atropos

Vangelis began as a developer from Greece. Six years ago he realized that only his dog didn't have an API, so he decided to steer his focus towards security.

That led him to pursue a PhD in Web Application Security with an extra focus on machine learning. He's still actively pursuing it.

He currently applies his skills as a Chief Technology Officer at Atropos, and during his free time, Vangelis is helping start-ups secure themselves on the internet and get a leg up in security terms.

His love of a simplistic approach to hacking by exploiting vulnerable APIs led him to publish research regarding API controlling ships, smart locks, IP cameras, car alarms, EV chargers, and many other IoT devices. Since our lives are nowadays extremely cyber-dependent, his goal is to convince all companies to never neglect their API security as rush-to-market mentality is almost certain to lead to catastrophic security failure.

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 15:30-15:59 PDT

Title: Ground Control to Major Threat - Hacking the Space Link Extension Protocol
When: Friday, Aug 9, 15:30 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Space missions have increasingly been the subject in the context of security breaches and satellite hacks. The majority of discussions revolve around direct communication and access to spacecraft through means such as Software Defined Radio. However, the reality is that this approach isn't practical for most adversaries, as it requires substantial resources and is easily detectable due to the power and radio frequencies required to command a spacecraft. Instead, adversaries might shift their focus away from the Space Segment and opt for a more practical approach, such as accessing and exploiting the Ground Segment vulnerabilities and flaws in order to gain control over spacecraft. Every space mission comprises custom-made hardware and software components, which interact with each other utilizing dedicated protocols and standards designed and developed for this sole purpose. Numerous potential failure points can adversely impact a space mission, many of which persist on the ground. Considering the essential services they facilitate and the extent to which contemporary society relies on space technology, each component utilized in space missions should be regarded as integral to critical infrastructure and treated as such, particularly from a security standpoint. This study centers on the Space Link Extension (SLE) protocol, which is employed as a standard for communication between mission data systems and ground stations by various space agencies and organizations, including NASA and ESA. We will address the security concerns inherent in the SLE protocol. At the same time, we demonstrate methods and techniques malicious actors can employ to conduct a Denial of Service (DoS) or tap into the ground station communications, gaining control over an actual spacecraft. We will conclude this publication by presenting the reader with a possible mitigation strategy that we believe should be employed at the SLE protocol level. Additionally, we will outline a forecast for future work, detailing both planned endeavors and those already in progress, to further expand on this research.

SpeakerBio: Andrzej Olchawa

Andy Olchawa is an experienced Information Security Professional with over 15 years in the space industry, working as a Software Engineer and Technical Project Manager. For the past few years, he has focused on offensive security, specializing in vulnerability research, exploit development, and red team operations. He holds OSCP, OSWA, and OSWP certifications, and has been credited with several CVEs.

Return to Index - Add to Google - ics Calendar file

CPV - Saturday - 17:30-17:59 PDT

Title: GUR RIBYHGVBA BS PELCGBTENCUL
When: Saturday, Aug 10, 17:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

I recently googled the meaning of “encryption” and found this definition on Wikipedia: “In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.” Um…no, encoding produces code, enciphering produces ciphertext, encryption is more than just encoding, and so on. Given the jumbling together of historically very unique and significant terminology I set out to find the actual, historical definitions and try to find a way to teach and/or demonstrate the differences in the foundational forms of cryptography. But I quickly noticed that some of this terminology is so often mis-applied in our digital age that I wondered if maybe there has been an evolution of the meanings of these terms? I might not like it, but I’m open to that possibility. This very quickly led me to the conclusion that my research on this topic would make for an interesting talk and so here we are. I want to share the classical, historical forms of cryptography, discuss the etymology of the terminology, look at how the words apply today – and help the audience decide if the actual meanings even matter (or it’s just me). One important consideration is the tradeoff between keeping the data secret (security) and protecting the identity of individuals associated with the data (privacy). I hope you’ll join me in this journey to victory (or defeat) in the ongoing battle of preserving the classic goals and objectives of data security.

SpeakerBio: Jeff Man

Jeff is a respected Information Security advocate, advisor, hacker, evangelist, mentor, teacher, international keynoter, speaker, former host of Security & Compliance Weekly, co-host on Paul's Security Weekly, Tribe of Hackers (TOH) contributor, including Red Team, Security Leaders, and Blue Team editions, and a member of the Cabal of the Curmudgeons. Jeff has over 40 years of experience working in all aspects of computer, network, and information security, including cryptography, risk management, vulnerability analysis, compliance assessment, forensic analysis and penetration testing. Certified National Security Agency Cryptanalyst. Designed and fielded the first software-based cryptosystem ever produced by NSA. Inventor of the "whiz" wheel, a cryptologic cipher wheel used by US Special Forces for over a decade currently on display at the National Cryptologic Museum. Honorary lifetime member of the Special Forces Association. Previously held security research, management and product development roles with the National Security Agency, the DoD and private-sector enterprises. Pioneering member of the first penetration testing "red team" at NSA. For the past twenty-eight years has been a pen tester, security architect, consultant, QSA, and PCI SME, providing consulting and advisory services to many of the nation's best known companies.

Return to Index - Add to Google - ics Calendar file

CON - Thursday - 12:00-12:59 PDT

Title: Hac-Man
When: Thursday, Aug 8, 12:00 - 12:59 PDT
Where: Virtual

Description:

Hybrid Contest On-site Hours: Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00 Becomes available online Thursday 12:00 Online and In-Person platforms will close Sunday 12:00 Players will only be able to turn in scavenger hunt items during On-site Hours.

This Pac-Man themed set of challenges takes Players on a journey through learning and demonstrating hacker and information security skills to earn points. With multiple subject-matter specific challenge groups and tracks, this hacker challenge game has something for everyone. You, dear Player, are Hac-Man (or Ms. Hac-Man, or Hac-Person), making your way through various dark mazes eating pellets, fruit, and ghosts. Each ghost represents a hacker puzzle or skills challenge. Upon completing each challenge, you'll be awarded points and can continue on to attempt further challenges. Many challenges have unlockable hints and location information, which you can unlock by spending your collected fruit.

There is a leaderboard! As you collect points, you'll show up on this leaderboard. The top 10 Players at the end of the game will be awarded various prizes from a prize pool.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Hac-Man
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-C - Map

Description:

Hybrid Contest On-site Hours: Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00 Becomes available online Thursday 12:00 Online and In-Person platforms will close Sunday 12:00 Players will only be able to turn in scavenger hunt items during On-site Hours.

This Pac-Man themed set of challenges takes Players on a journey through learning and demonstrating hacker and information security skills to earn points. With multiple subject-matter specific challenge groups and tracks, this hacker challenge game has something for everyone. You, dear Player, are Hac-Man (or Ms. Hac-Man, or Hac-Person), making your way through various dark mazes eating pellets, fruit, and ghosts. Each ghost represents a hacker puzzle or skills challenge. Upon completing each challenge, you'll be awarded points and can continue on to attempt further challenges. Many challenges have unlockable hints and location information, which you can unlock by spending your collected fruit.

There is a leaderboard! As you collect points, you'll show up on this leaderboard. The top 10 Players at the end of the game will be awarded various prizes from a prize pool.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Hac-Man
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-C - Map

Description:

Hybrid Contest On-site Hours: Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00 Becomes available online Thursday 12:00 Online and In-Person platforms will close Sunday 12:00 Players will only be able to turn in scavenger hunt items during On-site Hours.

This Pac-Man themed set of challenges takes Players on a journey through learning and demonstrating hacker and information security skills to earn points. With multiple subject-matter specific challenge groups and tracks, this hacker challenge game has something for everyone. You, dear Player, are Hac-Man (or Ms. Hac-Man, or Hac-Person), making your way through various dark mazes eating pellets, fruit, and ghosts. Each ghost represents a hacker puzzle or skills challenge. Upon completing each challenge, you'll be awarded points and can continue on to attempt further challenges. Many challenges have unlockable hints and location information, which you can unlock by spending your collected fruit.

There is a leaderboard! As you collect points, you'll show up on this leaderboard. The top 10 Players at the end of the game will be awarded various prizes from a prize pool.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Hac-Man
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-C - Map

Description:

Hybrid Contest On-site Hours: Friday and Saturday 10:00-18:00; Sunday: 10:00-12:00 Becomes available online Thursday 12:00 Online and In-Person platforms will close Sunday 12:00 Players will only be able to turn in scavenger hunt items during On-site Hours.

This Pac-Man themed set of challenges takes Players on a journey through learning and demonstrating hacker and information security skills to earn points. With multiple subject-matter specific challenge groups and tracks, this hacker challenge game has something for everyone. You, dear Player, are Hac-Man (or Ms. Hac-Man, or Hac-Person), making your way through various dark mazes eating pellets, fruit, and ghosts. Each ghost represents a hacker puzzle or skills challenge. Upon completing each challenge, you'll be awarded points and can continue on to attempt further challenges. Many challenges have unlockable hints and location information, which you can unlock by spending your collected fruit.

There is a leaderboard! As you collect points, you'll show up on this leaderboard. The top 10 Players at the end of the game will be awarded various prizes from a prize pool.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 15:30-16:30 PDT

Title: Haciendo visible lo invisible: Observabilidad y transparencia en routers Draytek
When: Saturday, Aug 10, 15:30 - 16:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Nuestra presentación se centra en cómo ganar observabilidad y transparencia a nivel de firmware en dispositivos que se encuentran el perímetro de la red. De esta forma, toca el tema central de DEF CON 32: Arreglar lo que esta roto en internet. Contaremos todo lo que aprendimos haciendo ingenieria inversa del firmware de los routers Draytek, cómo descubrimos vulnerabilidades que permiten ganar persistencia, y cómo aprovechamos esto para detectar posibles ataques de terceros sobre estos dispositivos. Mostraremos nuestro proceso y compartiremos nuestras herramientas para empoderar a los asistentes que deseen analizar estos routers, buscar nuevas vulnerabilidades, hardenearlos o incluso hacer mods que implementen nuevas funcionalidades.

Speakers: Gastón Aznarez,Octavio Gianatiempo

SpeakerBio: Gastón Aznarez, Security Researcher at Faraday

Gastón Aznarez is a computer enthusiast who is passionate about cybersecurity. He earned a degree in Computer Science and began working in malware detection in firmware. He currently works as a Security Researcher at Faraday, specializing in discovering and exploiting vulnerabilities in IoT and embedded devices. Gastón also participates in CTF competitions and has shared his expertise as a speaker at different conferences.

SpeakerBio: Octavio Gianatiempo, Student, Computer Science at University of Buenos Aires

Octavio Gianatiempo is a Security Researcher at Faraday and a Computer Science student at the University of Buenos Aires. He's also a biologist with research experience in molecular biology and neuroscience. The necessity of analyzing complex biological data was his point of entry into programming. However, he wanted to gain a deeper understanding of how computers work, so he enrolled in Computer Science. As a Security Researcher at Faraday, he focuses on vulnerability research on IoT and embedded devices and fuzzing open and closed-source software to find new vulnerabilities and exploit them. He has presented his findings at various conferences, including DEFCON, Ekoparty, 8.8, and Nerdearla.

Octavio Gianatiempo trabaja como Security Researcher en Faraday y es estudiante de Ciencias de la Computación en la Universidad de Buenos Aires. También es biólogo con experiencia en biología molecular y neurociencia. Dentro de su rol en Faraday, se enfoca en sistemas embebidos e IoT, ingeniería inversa y fuzzing de código abierto y propietario para identificar vulnerabilidades y explotarlas. Ha presentado sus hallazgos en conferencias como DEF CON, Ekoparty, 8.8 y Nerdearla.

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Hack My TV
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

With Google Cast Miracast or AirPlay smart TVs now have plenty of ways to get your favorite content on screen. But while the latest show is playing there is a complex system running underneath that is ripe for hacking. Bitdefender invites you to solve a few challenges that will get you diving into the inner workings of a smart TV.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Hack My TV
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

With Google Cast Miracast or AirPlay smart TVs now have plenty of ways to get your favorite content on screen. But while the latest show is playing there is a complex system running underneath that is ripe for hacking. Bitdefender invites you to solve a few challenges that will get you diving into the inner workings of a smart TV.

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Hack My TV
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

With Google Cast Miracast or AirPlay smart TVs now have plenty of ways to get your favorite content on screen. But while the latest show is playing there is a complex system running underneath that is ripe for hacking. Bitdefender invites you to solve a few challenges that will get you diving into the inner workings of a smart TV.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 11:00-11:59 PDT

Title: Hack the Badge (Badge class level 2) (Overflow if Friday is too full)
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

(NOTE: This is an overflow class only if the first session is full)

Learn how to hack the DCNextGen Badge and take it to another level!

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 14:00-14:59 PDT

Title: Hack the Badge (Badge class level 2)
When: Friday, Aug 9, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Learn how to hack the DCNextGen Badge and take it to another level!

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Hack-A-Sat Digital Twin
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Want to know what happened to the Hack-A-Sat digital twins? We're bringing back our satellites and ground stations so you can see what it was like to be a team operating during finals!

Establish uplink using a ground station. Send commands to the satellite, observe effects and telemetry. 3D Cesium visualization of satellite in orbit and ground station locations. Grafana dashboards for sim data, etc. OpenC3 satellite operator interface for C2

Speakers: Hack-A-Sat,Cromulence

SpeakerBio: Hack-A-Sat
No BIO available
SpeakerBio: Cromulence
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Hack-A-Sat Digital Twin
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Want to know what happened to the Hack-A-Sat digital twins? We're bringing back our satellites and ground stations so you can see what it was like to be a team operating during finals!

Establish uplink using a ground station. Send commands to the satellite, observe effects and telemetry. 3D Cesium visualization of satellite in orbit and ground station locations. Grafana dashboards for sim data, etc. OpenC3 satellite operator interface for C2

Speakers: Hack-A-Sat,Cromulence

SpeakerBio: Hack-A-Sat
No BIO available
SpeakerBio: Cromulence
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Hack-A-Sat Digital Twin
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Want to know what happened to the Hack-A-Sat digital twins? We're bringing back our satellites and ground stations so you can see what it was like to be a team operating during finals!

Establish uplink using a ground station. Send commands to the satellite, observe effects and telemetry. 3D Cesium visualization of satellite in orbit and ground station locations. Grafana dashboards for sim data, etc. OpenC3 satellite operator interface for C2

Speakers: Hack-A-Sat,Cromulence

SpeakerBio: Hack-A-Sat
No BIO available
SpeakerBio: Cromulence
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Hack-A-Sat Quals Challenges
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Enjoy some space math nostalgia with challenges from the past four years of Hack-A-Sat quals! Challenges require skills in astrodynamics, satellite operations, digital signal processing, reverse engineering, exploitation, and more! If you missed the last Hack-A-Sat qualifiers or just want to try again, now is your chance!

10 challenges are available with a mix of difficulty. These will be available throughout all of DEF CON so work on them anywhere (even your hotel room). No team required and no scoreboard...so no pressure!

Challenge developers will be available for hints/clues on the conference floor but may not be able to help with every challenge.

Speakers: Hack-A-Sat,Cromulence

SpeakerBio: Hack-A-Sat
No BIO available
SpeakerBio: Cromulence
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Hack-A-Sat Quals Challenges
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Enjoy some space math nostalgia with challenges from the past four years of Hack-A-Sat quals! Challenges require skills in astrodynamics, satellite operations, digital signal processing, reverse engineering, exploitation, and more! If you missed the last Hack-A-Sat qualifiers or just want to try again, now is your chance!

10 challenges are available with a mix of difficulty. These will be available throughout all of DEF CON so work on them anywhere (even your hotel room). No team required and no scoreboard...so no pressure!

Challenge developers will be available for hints/clues on the conference floor but may not be able to help with every challenge.

Speakers: Hack-A-Sat,Cromulence

SpeakerBio: Hack-A-Sat
No BIO available
SpeakerBio: Cromulence
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Hack-A-Sat Quals Challenges
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Enjoy some space math nostalgia with challenges from the past four years of Hack-A-Sat quals! Challenges require skills in astrodynamics, satellite operations, digital signal processing, reverse engineering, exploitation, and more! If you missed the last Hack-A-Sat qualifiers or just want to try again, now is your chance!

10 challenges are available with a mix of difficulty. These will be available throughout all of DEF CON so work on them anywhere (even your hotel room). No team required and no scoreboard...so no pressure!

Challenge developers will be available for hints/clues on the conference floor but may not be able to help with every challenge.

Speakers: Hack-A-Sat,Cromulence

SpeakerBio: Hack-A-Sat
No BIO available
SpeakerBio: Cromulence
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Friday - 14:00-15:59 PDT

Title: Hack3r Runw@y - Signups
When: Friday, Aug 9, 14:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/Contest Area - Map

Description:

Get ready to strut your stuff, hackers! We're thrilled to announce the 6th annual Hack3r Runw@y returning to DEF CON 32, bigger and bolder than ever.

Calling all glamorous geeks, crafty coders, and fashionably functional folks: Dust off your soldering irons, grab your needles and threads, and unleash your creativity! Hack3r Runw@y challenges you to reimagine fashion through the lens of hacking.

Show us your wearable tech wonders in the following 4 categories for a chance to win in each category plus one coveted People’s Choice trophy where ANYONE can win, but there will be a twist. Did you see this year's theme (hint).

Smart wear that wows: Integrate LEDs, microcontrollers, and sensors into your designs for dazzling functionality.

Digital design that dazzles: light it up with LEDs, bling with lights, but keep it passive.

Functional Fashion: masks and shields, hazmat suit, lockpick earrings, and cufflink shims.

Extraordinary style: Elevate your daily wardrobe with unique fabrics, passive design, 3d textures, optical illusions, cosplay, and security-inspired patterns.

No matter your skill level, Hack3r Runw@y has a place for you! Whether you're a seasoned maker or a coding newbie, join us in celebrating the convergence of creativity, technology, and style.

Winners selected by judges selection based on:

Uniqueness Trendy Practical Couture Creativity Relevance Originality Presentation Mastery

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 13:00-14:59 PDT

Title: Hack3r Runw@y
When: Saturday, Aug 10, 13:00 - 14:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

Get ready to strut your stuff, hackers! We're thrilled to announce the 6th annual Hack3r Runw@y returning to DEF CON 32, bigger and bolder than ever.

Calling all glamorous geeks, crafty coders, and fashionably functional folks: Dust off your soldering irons, grab your needles and threads, and unleash your creativity! Hack3r Runw@y challenges you to reimagine fashion through the lens of hacking.

Show us your wearable tech wonders in the following 4 categories for a chance to win in each category plus one coveted People’s Choice trophy where ANYONE can win, but there will be a twist. Did you see this year's theme (hint).

Smart wear that wows: Integrate LEDs, microcontrollers, and sensors into your designs for dazzling functionality.

Digital design that dazzles: light it up with LEDs, bling with lights, but keep it passive.

Functional Fashion: masks and shields, hazmat suit, lockpick earrings, and cufflink shims.

Extraordinary style: Elevate your daily wardrobe with unique fabrics, passive design, 3d textures, optical illusions, cosplay, and security-inspired patterns.

No matter your skill level, Hack3r Runw@y has a place for you! Whether you're a seasoned maker or a coding newbie, join us in celebrating the convergence of creativity, technology, and style.

Winners selected by judges selection based on:

Uniqueness Trendy Practical Couture Creativity Relevance Originality Presentation Mastery

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-B - Map

Description:

We would like to see cancer become a thing of the past, and you can help. How? Join the Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge. Here's how it works:

1. Accept our Challenge. If you accept the Challenge, you're also committing to nominate three people to join you.
2. Take a video of yourself dumping a bucket of ice water over your head in combination with a Contraption of your construction to lower your temperature and raise awareness of cancer. Trust us, it's way easier to do this during the summer in Vegas than at Halifax Analytica headquarters in the winter.
3. Post the audio to the TeleChallenge voice BBS challenging up to three others using their phone number, or post a video to https://defcon.social or your social media of choice using the hashtag #HackerCoolingContraption and the following:
    - Your handle
    - Who challenged you
    - A statement of acceptance ("I agree that I am responsible for my own hacker cooling actions, I understand that water is wet, and I promise not to sue the TeleChallenge or DEF CON" or something to that effect)
    - The handles of 3 people you are nominating
    - A link to a nonprofit cancer research project or charity of your choice that you have chosen to support
    - A mention of your contribution (including cash, cryptocurrency, volunteer hours, or computing resources), if any

Suggested: Make a contribution of your choice to support cancer research. You may want to check nonprofit and charity quality here: https://www.charitynavigator.org/

RULES

1. You can use up to 4 items obtained either from the TeleChallenge booth or at a dollar store costing no more than $5 plus tax, plus duct tape, along with a single one-gallon bucket or container full of conventional ice and water (solely H2O!) to build your Contraption.
2. Only hand tools may be used.
3. No hackers may be harmed in the execution of the Challenge. Contraption may cool to no colder than -3 degrees Celcius.
4. You may wear no less than a bathing suit (due to dress code requirements at pools).
5. Contraptions will be judged only for full participants of the Challenge, meaning you have made three nominations and at least two nominees have also participated.
6. Judging criteria: Efficacy, creativity, flair, hax.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-B - Map

Description:

We would like to see cancer become a thing of the past, and you can help. How? Join the Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge. Here's how it works:

1. Accept our Challenge. If you accept the Challenge, you're also committing to nominate three people to join you.
2. Take a video of yourself dumping a bucket of ice water over your head in combination with a Contraption of your construction to lower your temperature and raise awareness of cancer. Trust us, it's way easier to do this during the summer in Vegas than at Halifax Analytica headquarters in the winter.
3. Post the audio to the TeleChallenge voice BBS challenging up to three others using their phone number, or post a video to https://defcon.social or your social media of choice using the hashtag #HackerCoolingContraption and the following:
    - Your handle
    - Who challenged you
    - A statement of acceptance ("I agree that I am responsible for my own hacker cooling actions, I understand that water is wet, and I promise not to sue the TeleChallenge or DEF CON" or something to that effect)
    - The handles of 3 people you are nominating
    - A link to a nonprofit cancer research project or charity of your choice that you have chosen to support
    - A mention of your contribution (including cash, cryptocurrency, volunteer hours, or computing resources), if any

Suggested: Make a contribution of your choice to support cancer research. You may want to check nonprofit and charity quality here: https://www.charitynavigator.org/

RULES

1. You can use up to 4 items obtained either from the TeleChallenge booth or at a dollar store costing no more than $5 plus tax, plus duct tape, along with a single one-gallon bucket or container full of conventional ice and water (solely H2O!) to build your Contraption.
2. Only hand tools may be used.
3. No hackers may be harmed in the execution of the Challenge. Contraption may cool to no colder than -3 degrees Celcius.
4. You may wear no less than a bathing suit (due to dress code requirements at pools).
5. Contraptions will be judged only for full participants of the Challenge, meaning you have made three nominations and at least two nominees have also participated.
6. Judging criteria: Efficacy, creativity, flair, hax.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-B - Map

Description:

We would like to see cancer become a thing of the past, and you can help. How? Join the Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge. Here's how it works:

1. Accept our Challenge. If you accept the Challenge, you're also committing to nominate three people to join you.
2. Take a video of yourself dumping a bucket of ice water over your head in combination with a Contraption of your construction to lower your temperature and raise awareness of cancer. Trust us, it's way easier to do this during the summer in Vegas than at Halifax Analytica headquarters in the winter.
3. Post the audio to the TeleChallenge voice BBS challenging up to three others using their phone number, or post a video to https://defcon.social or your social media of choice using the hashtag #HackerCoolingContraption and the following:
    - Your handle
    - Who challenged you
    - A statement of acceptance ("I agree that I am responsible for my own hacker cooling actions, I understand that water is wet, and I promise not to sue the TeleChallenge or DEF CON" or something to that effect)
    - The handles of 3 people you are nominating
    - A link to a nonprofit cancer research project or charity of your choice that you have chosen to support
    - A mention of your contribution (including cash, cryptocurrency, volunteer hours, or computing resources), if any

Suggested: Make a contribution of your choice to support cancer research. You may want to check nonprofit and charity quality here: https://www.charitynavigator.org/

RULES

1. You can use up to 4 items obtained either from the TeleChallenge booth or at a dollar store costing no more than $5 plus tax, plus duct tape, along with a single one-gallon bucket or container full of conventional ice and water (solely H2O!) to build your Contraption.
2. Only hand tools may be used.
3. No hackers may be harmed in the execution of the Challenge. Contraption may cool to no colder than -3 degrees Celcius.
4. You may wear no less than a bathing suit (due to dress code requirements at pools).
5. Contraptions will be judged only for full participants of the Challenge, meaning you have made three nominations and at least two nominees have also participated.
6. Judging criteria: Efficacy, creativity, flair, hax.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 20:00-21:59 PDT

Title: Hacker Jeopardy
When: Saturday, Aug 10, 20:00 - 21:59 PDT
Where: LVCC West/Floor 1/Hall 1/Tracks 1-2 - Map

Description:

Return to Index - Add to Google - ics Calendar file

CON - Friday - 20:00-21:59 PDT

Title: Hacker Jeopardy
When: Friday, Aug 9, 20:00 - 21:59 PDT
Where: LVCC West/Floor 1/Hall 1/Tracks 1-2 - Map

Description:

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 20:00-01:59 PDT

Title: Hacker Karaoke
When: Saturday, Aug 10, 20:00 - 01:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

We are the event to go to if you want to hang out, enjoy the festivities, sing along, and show ones hidden talent.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 20:00-01:59 PDT

Title: Hacker Karaoke
When: Friday, Aug 9, 20:00 - 01:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

We are the event to go to if you want to hang out, enjoy the festivities, sing along, and show ones hidden talent.

Return to Index - Add to Google - ics Calendar file

PLV - Saturday - 13:15-13:59 PDT

Title: Hacker vs AI: perspectives from an ex-spy
When: Saturday, Aug 10, 13:15 - 13:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

The convergence of Artificial Intelligence (AI) and national security not only fuels international discourse but also inspires narratives within popular culture. Harriet is no stranger to these myths, as an ex-intelligence professional who specialized in applying machine learning to cyber security. In fact, she likes to lean into them. This makes her previous bosses nervous, so she uses pop culture as the lens through which to communicate her insights - and in this talk she utilizes the worlds of Ghost in the Shell, Neuromancer and Mission Impossible.

Through these stories, as well as her own decade of experience working at the intersection of artificial intelligence and cyber security, Harriet discusses the extent to which fears surrounding AI systems are applicable to real life national security settings. From cyber warfare to AI-driven surveillance, she unravels the interplay between hackers, AI, and government agencies. This session is interactive, with demos of how these AI systems actually work under the hood, as well as discussion time. Blur the lines between human and machine, and understand how you can contribute your skills to prevent our own modern day Puppet Master.

SpeakerBio: Harriet Farlow, CEO at Mileva Security Labs

Harriet Farlow is the CEO of AI Security company Mileva Security Labs, a PhD Candidate in Machine Learning Security, and creative mind behind the YouTube channel HarrietHacks. She missed the boat on computer hacking so now she hacks AI and Machine Learning models instead. Her career has spanned consulting, academia, a start-up and Government, but don't judge her for that one. She also has a Bachelor in Physics and a Master in Cyber Security. She calls Australia home but has lived in the UK and the US. Her ultimate hack was in founding her own AI Security company but if Skynet takes over she will deny everything and pretend the AI stood for Artificial Insemination, like her Mum thinks it does. (Sorry Mum but I'm not really a Medical Doctor).

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: HackFortress
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-A - Map

Description:

Friday: Free play 10:00 - 15:00,
Prelim Round 1: 16:00 - 17:00,
Prelim Round 2: 17:00 - 18:00,
Registration closes: 18:00

Saturday: Prelim Round 3: 11:00, Prelim Round 4: 12:00, Semi Finals Round 1: 14:00, Semi Finals Round 2: 15:00, Finals: 17:00

HackFortress is a unique blend of Team Fortress 2 and a computer security contest. Teams are made up of 6 TF2 players and 4 hackers. TF2 players duke it out while hackers are busy with challenges like application security, network security, social engineering, or reverse engineering. As teams start scoring they can redeem points in the hack fortress store for bonuses. Bonuses range from crits for the TF2, lighting the opposing team on fire, or preventing the other teams hackers from accessing the store. HackFortress challenges range from beginner to advanced, from serious to absurd.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: HackFortress
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-A - Map

Description:

Friday: Free play 10:00 - 15:00,
Prelim Round 1: 16:00 - 17:00,
Prelim Round 2: 17:00 - 18:00,
Registration closes: 18:00

Saturday: Prelim Round 3: 11:00, Prelim Round 4: 12:00, Semi Finals Round 1: 14:00, Semi Finals Round 2: 15:00, Finals: 17:00

HackFortress is a unique blend of Team Fortress 2 and a computer security contest. Teams are made up of 6 TF2 players and 4 hackers. TF2 players duke it out while hackers are busy with challenges like application security, network security, social engineering, or reverse engineering. As teams start scoring they can redeem points in the hack fortress store for bonuses. Bonuses range from crits for the TF2, lighting the opposing team on fire, or preventing the other teams hackers from accessing the store. HackFortress challenges range from beginner to advanced, from serious to absurd.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 13:00-17:59 PDT

Title: Hacking Boundary Terminal
When: Saturday, Aug 10, 13:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-E - Map

Description:

In this MarSec event we will engage convention goers with a number of different tabletop games to help them understand the operational issues surrounding offensive and defensive cyber operations in a port complex. Players will become familiar with the various network components that support port and shipping operations from the underlying infrastructure to the system components at ports and commercial ships. A fictional terminal, Boundary Terminal part of the Port Elizabeth New Jersey complex, and a fictional shipping line, Worldwide Shipping Operations form the basis for all of three of our games. The games are: a short game designed to show the basic target set and linkages, a longer role-playing game where players can engage in detail with port systems, and a card driven game focused on detection, forensics, and counter-forensics. The role-playing game has been conducted as part of the MarSec portion of the ICS Village for the past two years, while the shorter version was added last year. This year we will add the counter-forensics game. All of the games are designed to be entertaining and engaging with prizes provided to the winners and best players (usually everyone gets a prize).

Return to Index - Add to Google - ics Calendar file

CON - Friday - 13:00-17:59 PDT

Title: Hacking Boundary Terminal
When: Friday, Aug 9, 13:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-E - Map

Description:

In this MarSec event we will engage convention goers with a number of different tabletop games to help them understand the operational issues surrounding offensive and defensive cyber operations in a port complex. Players will become familiar with the various network components that support port and shipping operations from the underlying infrastructure to the system components at ports and commercial ships. A fictional terminal, Boundary Terminal part of the Port Elizabeth New Jersey complex, and a fictional shipping line, Worldwide Shipping Operations form the basis for all of three of our games. The games are: a short game designed to show the basic target set and linkages, a longer role-playing game where players can engage in detail with port systems, and a card driven game focused on detection, forensics, and counter-forensics. The role-playing game has been conducted as part of the MarSec portion of the ICS Village for the past two years, while the shorter version was added last year. This year we will add the counter-forensics game. All of the games are designed to be entertaining and engaging with prizes provided to the winners and best players (usually everyone gets a prize).

Return to Index - Add to Google - ics Calendar file

APV - Friday - 12:30-12:59 PDT

Title: Hacking Corporate Banking for Fun and Profit
When: Friday, Aug 9, 12:30 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

I conducted thorough research on a corporate banking software widely utilized by numerous banks globally. This research was conducted during a bug bounty program for a leading bank in middle east, which employs this software. By examining their marketing brochures, we identified the third party company responsible for its development and after looking at their client we found out, their software is utilized by 60-70% of banks worldwide.

In this talk i will explain how did i recon corporate banking application from extracting interesting endpoints and methods. Further used them to find attack surface. Furthermore, I will delve into the methods used to uncover critical vulnerabilities within their application, including SQL injections, bypassing access control mechanisms etc.

Speakers: Charles Waterhouse,Nikhil "niks" Shrivastava

SpeakerBio: Charles Waterhouse

After spending over 2 decades in the airline industry, I changed careers into cybersecurity. I have helped manage over 2400 engagements with teams of over 1000 researchers across all verticals in commercialand government. I regularly consult with executives in many Global 500 organizations and government to developsecurity and testing plans.

I have helped develop products around OWASP, NIST, OSINT, API and AI testing. I speak regularly at conferences and help train developers and blue teams to help defend some of the most critical networks worldwide.

SpeakerBio: Nikhil "niks" Shrivastava

My Name is Nikhil Shrivastava AKA niksthehacker. I am an ethical hacker and bug bounty hunter. I have helped over 300 companies to uncover 1500+ Security Vulnerabilities such as Google, Microsoft, Tesla, Mozilla, Salesforce, eBay, Federal Agencies, and many more. I am the #1 hacker in India at Synack Red Team. I was awarded "Synack Legend Hacker" Status in 2021. I have also been interviewed by Defcon Red Team Village, Synack, and Indian media such as the Times of India, Economic Times, Indian Express, etc. I was also MSRC (Microsoft Security Response Center) Top 100 Hackers in 2016. I am the founder of Security BSides Ahmedabad, an international hacking conference hosted each year in Ahmedabad, India.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 14:00-14:45 PDT

Title: Hacking Millions of Modems (and Investigating Who Hacked My Modem)
When: Saturday, Aug 10, 14:00 - 14:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

On December 25th, 2021, I discovered that my modem had been hacked after a strange IP address replayed my traffic. I began researching who they were, how it happened, and eventually discovered a vulnerability which allowed me to passively monitor, change configurations, and execute commands on millions of devices. This talk details 3 years of intermittent web research on ISP security and how broadband equipment is becoming scarily centralized.

1. N. Mavrakis, "Vulnerabilities of ISPs," in IEEE Potentials, vol. 22, no. 4, pp. 9-15, Oct.-Nov. 2003, doi: 10.1109/MP.2003.1238687
2. I Hunt TR-069 Admins: Pwning ISPs Like a Boss (Shahar Tal, August 2014, link)
3. TR-069 Wikipedia link
4. Cox Communications VDP link

SpeakerBio: Sam Curry, Founder at Palisade

Sam Curry is a web security researcher, bug bounty hunter, and the founder of Palisade, a security consultancy.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 16:00-16:50 PDT

Title: Hacking Policy and Policy Hacking - A Red-Teamer Hacker Guide to the Universe of Cyber Policy
When: Saturday, Aug 10, 16:00 - 16:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

Cybersecurity Policy has transformed red teaming. Cyber and AI are the most emerging domains of the law, with strategies, regulations, and standards constantly emerging, globally. This domain also serves as an amazing opportunity for you explore to new paths, and opportunities, to drive impact at scale, and collaborate with the hacker ecosystem to drive better policies, and better security – that advance all users. This talk invites the audience to explore the latest trend in cyber policy globally, focusing on areas with broad impact on the red teaming community – such as AI red teaming, pen testing policy, secure development, legal limitations to vuln disclosure, and anti-hacking laws. We will cover the latest developments from CIRCIA to the EU Cyber Resilience Act and the AI EO – and introduce the audience to the world of policy hacking, and policy "hacking". We will cover case studies and

SpeakerBio: Amit Elazari
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 10:00-10:50 PDT

Title: Hacking Processes: Introducing the Redteaming Process Framework: RTPF
When: Sunday, Aug 11, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

People often talk about red teaming as hacking people or systems, but no one really talks about hacking processes. Company processes are oftentimes some of the most critical business functions that a threat actor could go after, but there is no framework or attack chain lifecycle equivalent for red teaming processes. In this talk, we'll be talking about how Fortune 500 red teamers simulate adversaries and attack processes, and how you can use our new framework, the Redteaming Process Framework: RTPF, to do the same.

Speakers: Alex Gonzalez,Bobby R

SpeakerBio: Alex Gonzalez
No BIO available
SpeakerBio: Bobby R
No BIO available

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 11:00-11:59 PDT

Title: Hacking Quantum Key Distribution (QKD)
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Quantum cryptography is unbreakable in principle but suffers from implementation vulnerabilities that may compromise the perfect protocol. I show examples of such vulnerabilities and tell about upcoming certification standards that verify the quality of countermeasures.

SpeakerBio: Vadim Makarov

Vadim received his M.Sc from St. Petersburg State Polytechnical University in 1998. He obtained a Doctor Engineer Degree in Physics Electronics at the Norwegian University of Science and Technology in 2007. After postdoctoral positions at Pohang University of Science and Technology (South Korea) and at the Norwegian University of Science and Technology, in 2012 he joined the Institute for Quantum Computing, Waterloo University (Canada) as research Assistant Professor. Since 2018 he is an applied PI at the Russian Quantum Center, and Professor at the National University of Science and Technology MISiS in Moscow since 2019. In 2023, he joined the Vigo Quantum Communication Center as group leader of the Quantum Hacking & Certification Lab. His research interest lies in quantum communication, particularly quantum hacking.

Return to Index - Add to Google - ics Calendar file

HRV - Friday - 14:00-14:59 PDT

Title: Hacking the Quansheng UV-K5
When: Friday, Aug 9, 14:00 - 14:59 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

The Quansheng UV-K5 has quickly become the hot new budget radio for new hams and old hams that love to tinker. In this presentation, I will talk about the capabilities of the radio, open source firmware mods, and hardware mods. I'll also show why transmitting with a radio on frequencies it can't properly filter can be a bad idea!

SpeakerBio: Jon Marler
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 10:00-10:50 PDT

Title: Hacking the Skies – Satellite Red Teaming
When: Saturday, Aug 10, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

Satellites form a critical infrastructure for our modern world, enabling global communications, navigation, weather forecasting, and more. However, the growing reliance on satellites also highlights a troubling concern: their cybersecurity vulnerabilities.

Firstly, I provide a technical overview of how satellite communications work, covering aspects such as signal transmission, encryption, and decryption. This leads into an examination of vulnerabilities, including insecure communication channels, outdated encryption algorithms, and hardware flaws, which can be exploited by malicious actors.

Then shift focus to the practical aspects of satellite hacking, outlining key methods such as signal interception, replay attacks, and jamming. We introduce essential tools for these tasks, including GNU Radio, SDR (Software-Defined Radio), that will be used practically.

Case studies are also discussed, providing insights into high-profile satellite hacking incidents. These real-world examples and personal war stories serve to highlight the various methods used, lessons learned, and challenges faced by red teams in this domain, including signal interference and staying ahead of security updates. The paper concludes with guidance for red teams and cybersecurity professionals. I offer advice on setting up a satellite hacking environment, conducting effective penetration testing, and reporting findings.

In summary, this talk aims to illuminate the vulnerabilities of satellite systems and provide red teams with the technical, ethical, and practical knowledge necessary to navigate this unique domain responsibly.

SpeakerBio: Agostino Panico
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Hacking the Vote: How Hackers Caused the Downfall of the Dutch Voting Machines
When: Friday, Aug 9, 17:00 - 17:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

It's 2007 when the Dutch Ministry of Internal Affairs orders a ban on voting machines. Voting machines that have been in use for over a decade by then. The reason? The Dutch Secret Service has declared the TEMPEST radiation emitted by the voting machines makes it possible for someone outside the polling station to see what someone is voting. But that is just the tip of the voting machine-ice berg. What came before is two years of a foundation started by a group off Dutch hackers that fought to prove that voting machines in their current form are unreliable, cannot be checked and can be manipulated to show any result you want, regardless of the votes that are given as input. What followed is a lengthy report of a government ordered commission that describes 8 principles of trustworthy elections. These principles are very difficult to adhere to using voting machines, even modern voting machines. The reason for this are some fundamental issues that come with computers: a lack of transparency for those without a technical background as well as the issue of voting secrecy (nobody being able to tell what a specific person voted for). In this presentation; I outline the history of the Dutch voting machines and their demise, what a group of hackers had to do with this, as well as the fundamental issues that we still struggle with to this day. Listeners can take this information as lessons for their own election processes. Mind you, we are not saying not to use voting machines. We are not against the idea of voting machines. However, the issues we as the Netherlands are struggling with have still not been resolved to this very day.

SpeakerBio: Fleur van Leusden

Fleur van Leusden is an experienced CISO working for various Dutch government organizations in the past decade. She has done research on security in cars using autonomous driving software as well as working for the Amsterdam police department as an internet detective. She currently works for the Dutch Electoral Council as their first ever CISO, where her job is to keep the election process in the Netherlands secure. This government body has existed for over 100 years and is responsible for organizing the elections in the Netherlands as well as advising around law and other matters surrounding the subject.

Return to Index - Add to Google - ics Calendar file

HRV - Thursday - 10:00-16:59 PDT

Title: Ham in a Day Class
When: Thursday, Aug 8, 10:00 - 16:59 PDT
Where: Other / See Description

Description:

Learn and earn your Amateur (Ham) License @ DEF CON 32 with this free class offered by Dan KB6NU and the Ham Radio Village!

Always been interested in getting your ham license but never had the time to study? Now's your chance! The Ham Radio Village is offering a one-day class where you can learn all the required knowledge to pass the exam.

Topics include: - Electrical Principles - Electronic principles and components - Radio and electromagnetic wave properties - Antennas and Feedlines - Amateur Radio Signals - Safety - Station Setup and Operation - Operating Procedures - Rules and Regulations

After the class, you can earn your license by taking the exam (for free) at DEF CON on your choice of Friday, Saturday, or Sunday. (Online testing is also available post-conference)

The class will run from 10 A.M. to 5 P.M. on Thursday, August 8th at the Clark County Library** located nearby to the LVCC at 1401 E Flamingo Rd. A lunch break will be provided.

Best of all, this class is completely free, thanks to a grant from the Amateur Radio Digital Communications.

Last year, we sold out of capacity and had to turn folks away. We highly recommend placing a deposit to reserve your seat. The deposit will be refunded upon attendance of the class.

Note: this event is not located at the Las Vegas Convention Center but at the nearby Clark County Library. If you're planning on taking public transit, it is directly served by bus routes CX, 109, 202. Free parking (with EV charging) is available onsite.

Clark County Library, 1401 E Flamingo Rd, Las Vegas, NV 89119 Google Maps Apple Maps

This program is not a Library District event. The views expressed and other information presented are solely those of the producing entity.

SpeakerBio: Dan "dan_kb6nu" Romanchik, Ham Radio Village
No BIO available

Return to Index - Add to Google - ics Calendar file

HRV - Saturday - 11:00-16:59 PDT

Title: Ham Radio Exams
When: Saturday, Aug 10, 11:00 - 16:59 PDT
Where: LVCC West/Floor 3/W320 - Map

Description:

Ham radio is the original group of electronic hackers, starting long before computers, circuit chips, or even transistors. Continuing this pioneer spirit, The Ham Radio Village is offering free ham radio exams again at DEF CON! All are welcome to come and take the exam and get their amateur radio license upon passing. All three levels (technician, general, and amateur extra) of exams will be offered during DEF CON at the Ham Radio Village. Examinees are encouraged to study the question pool and take practice exams on ham.study.

Everything we do today involves wireless communications of some sort, and a basic knowledge of how radio works is crucial. Getting your amateur radio license and entering the world of amateur radio will better equip you with knowledge about what goes on in the radio frequency domain, and this can be applied to other RF topics (like RFID credentials, WiFi, or anything else that communicated wirelessly)

Return to Index - Add to Google - ics Calendar file

HRV - Friday - 13:00-15:59 PDT

Title: Ham Radio Exams
When: Friday, Aug 9, 13:00 - 15:59 PDT
Where: LVCC West/Floor 3/W320 - Map

Description:

Ham radio is the original group of electronic hackers, starting long before computers, circuit chips, or even transistors. Continuing this pioneer spirit, The Ham Radio Village is offering free ham radio exams again at DEF CON! All are welcome to come and take the exam and get their amateur radio license upon passing. All three levels (technician, general, and amateur extra) of exams will be offered during DEF CON at the Ham Radio Village. Examinees are encouraged to study the question pool and take practice exams on ham.study.

Everything we do today involves wireless communications of some sort, and a basic knowledge of how radio works is crucial. Getting your amateur radio license and entering the world of amateur radio will better equip you with knowledge about what goes on in the radio frequency domain, and this can be applied to other RF topics (like RFID credentials, WiFi, or anything else that communicated wirelessly)

Return to Index - Add to Google - ics Calendar file

HRV - Sunday - 10:00-13:30 PDT

Title: Ham Radio Exams
When: Sunday, Aug 11, 10:00 - 13:30 PDT
Where: LVCC West/Floor 3/W320 - Map

Description:

Ham radio is the original group of electronic hackers, starting long before computers, circuit chips, or even transistors. Continuing this pioneer spirit, The Ham Radio Village is offering free ham radio exams again at DEF CON! All are welcome to come and take the exam and get their amateur radio license upon passing. All three levels (technician, general, and amateur extra) of exams will be offered during DEF CON at the Ham Radio Village. Examinees are encouraged to study the question pool and take practice exams on ham.study.

Everything we do today involves wireless communications of some sort, and a basic knowledge of how radio works is crucial. Getting your amateur radio license and entering the world of amateur radio will better equip you with knowledge about what goes on in the radio frequency domain, and this can be applied to other RF topics (like RFID credentials, WiFi, or anything else that communicated wirelessly)

Return to Index - Add to Google - ics Calendar file

HRV - Saturday - 11:00-11:59 PDT

Title: Ham Radio for Hackers
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

Lots of fun things are happening in amateur radio for those who like to hack on hardware and software. This talk is an introduction to some of them.

SpeakerBio: Dan "dan_kb6nu" Romanchik, Ham Radio Village
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:30-17:59 PDT

Title: Ham Radio Fox Hunt
When: Friday, Aug 9, 10:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-A - Map

Description:

This contest is simple, and is designed to teach you the basics of transmitter direction finding and “fox hunting”. We offer multiple levels of difficulty – whether you’ve never done a fox hunt before or are a seasoned pro, you can participate in the hunt! Learning how to locate the source of radio signals is an important tool you can add to your hacker arsenal. Whether you’re hunting for a source of interference, a rogue wireless AP, or tracking down the FCC’s monitoring vans, the real-world skills you will gain from this contest will be invaluable.

To participate in the beginner IR foxhunt you will need a device that can receive IR light in the 900nm range – such as many cell phones and digital cameras!

To participate in the RF foxhunt(s) you will need a radio or a scanner that can receive signals in the 2m and/or 70cm Amateur Radio Bands (144.000 MHz - 146.000 MHz, 420.000 MHZ - 450.000 MHz)

SpeakerBio: Ham Radio Village Staff
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Ham Radio Fox Hunt
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-A - Map

Description:

This contest is simple, and is designed to teach you the basics of transmitter direction finding and “fox hunting”. We offer multiple levels of difficulty – whether you’ve never done a fox hunt before or are a seasoned pro, you can participate in the hunt! Learning how to locate the source of radio signals is an important tool you can add to your hacker arsenal. Whether you’re hunting for a source of interference, a rogue wireless AP, or tracking down the FCC’s monitoring vans, the real-world skills you will gain from this contest will be invaluable.

To participate in the beginner IR foxhunt you will need a device that can receive IR light in the 900nm range – such as many cell phones and digital cameras!

To participate in the RF foxhunt(s) you will need a radio or a scanner that can receive signals in the 2m and/or 70cm Amateur Radio Bands (144.000 MHz - 146.000 MHz, 420.000 MHZ - 450.000 MHz)

SpeakerBio: Ham Radio Village Staff
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Ham Radio Fox Hunt
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-A - Map

Description:

This contest is simple, and is designed to teach you the basics of transmitter direction finding and “fox hunting”. We offer multiple levels of difficulty – whether you’ve never done a fox hunt before or are a seasoned pro, you can participate in the hunt! Learning how to locate the source of radio signals is an important tool you can add to your hacker arsenal. Whether you’re hunting for a source of interference, a rogue wireless AP, or tracking down the FCC’s monitoring vans, the real-world skills you will gain from this contest will be invaluable.

To participate in the beginner IR foxhunt you will need a device that can receive IR light in the 900nm range – such as many cell phones and digital cameras!

To participate in the RF foxhunt(s) you will need a radio or a scanner that can receive signals in the 2m and/or 70cm Amateur Radio Bands (144.000 MHz - 146.000 MHz, 420.000 MHZ - 450.000 MHz)

SpeakerBio: Ham Radio Village Staff
No BIO available

Return to Index - Add to Google - ics Calendar file

HRV - Saturday - 16:00-16:30 PDT

Title: Ham Radio in an HOA: Radio in the Face of Your Oppressor
When: Saturday, Aug 10, 16:00 - 16:30 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

Home Owners Association or HOAs make amateur radio difficult. The good antennas are restricted, requiring a little bit of compromise and creativity to work around. This talk is how I worked around my HOA's covenants, conditions, and restrictions to operate my antenna.

This talk will present actual proven techniques to allow you to operate on all the amateur bands. I will talk about my personal horizontal loop deployment, as well as talk about all the bad antenna options I tried first before getting here.

SpeakerBio: Danny Quist
No BIO available

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 13:00-13:25 PDT

Title: HandPwning: "Your Hand is your Passport. Verify me. Now let me in!"
When: Friday, Aug 9, 13:00 - 13:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

Biometrics applied to PACS (Physical Access Control Systems) has been an hot-topic for a few years now. The spread of fingerprint or face recognition based access control and time attendance systems among corporate, industrial and military environments has surged. And with it, also the number of potential attack vectors has increased. In this talk, after a brief overview of the state of art of available PACS utilizing biometrics to authenticate and authorize users, we will investigate one technology among others (usually perceived less-invasive) that has been widely used in some specific fields (e.g. industrial plants, airports, food industry, etc.): the handpunch access control and time attendance systems. The handpunch PACS are based on the hand-geometry recognition. In this presentation we will have a look how this tech works and, in particular, we will focus our attention on reviewing some of existing handpunch devices: from a physical security POV until reversing the communication protocol. Moreover, during the presentation will be demonstrated how to remotely push a new super-admin user into it (i.e. persistent backdoor), how to dump existing users credentials and will be also released an opensource tool-suite: HandScan & HandPwner.

Eventually, thanks the cooperation with Shodan's creator, it has been confirmed that more than 1800 of these vulnerable devices were found exposed on the Internet. Finally, we will conclude the talk with practical and actionable countermeasures to prevent these attacks and how to harden these devices.

SpeakerBio: Luca "CYBERANTANI" Bongiorni, Founder at We Hack In Disguise (WHID)
Luca Bongiorni is working as Director of a CyberSecurity Lab and is Founder of WHID - We Hack In Disguise: a cybersecurity boutique focused on R&D offensive hardware implants and IIoT Security. Luca is also actively involved in InfoSec where his main fields of research are: Radio Networks, Hardware Hacking, Internet of Things, and Physical Security. At the moment, he is focusing his researches on bypassing biometric access control systems, IIoT Security & Forensics, Air-Gapped Environments and IoOT (Internet of Offensive Things).

Return to Index - Add to Google - ics Calendar file

PSV - Sunday - 11:30-11:59 PDT

Title: HandPwning: “Your Hand is your Passport. Verify me. Now let me in!”
When: Sunday, Aug 11, 11:30 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Biometrics applied to PACS (Physical Access Control Systems) has been an hot-topic for a few years now. The spread of fingerprint or face recognition based access control and time attendance systems among corporate, industrial and military environments has surged. And with it, also the number of potential attack vectors has increased. In this talk, after a brief overview of the state of art of available PACS utilizing biometrics to authenticate and authorize users, we will investigate one technology among others (usually perceived less-invasive) that has been widely used in some specific fields (e.g. industrial plants, airports, food industry, etc.): the handpunch access control and time attendance systems. The handpunch PACS are based on the hand-geometry recognition. In this presentation we will have a look how this tech works and, in particular, we will focus our attention on reviewing some of existing handpunch devices: from a physical security POV until reversing the communication protocol. Moreover, during the presentation will be demonstrated how to remotely push a new super-admin user into it (i.e. persistent backdoor), how to dump existing users credentials and will be also released an opensource tool-suite: HandScan & HandPwner. Eventually, thanks the cooperation with Shodan’s creator, it has been confirmed that more than 1800 of these vulnerable devices were found exposed on the Internet. Finally, we will conclude the talk with practical and actionable countermeasures to prevent these attacks and how to harden these devices.

SpeakerBio: Luca "CYBERANTANI" Bongiorni, Founder at We Hack In Disguise (WHID)
Luca Bongiorni is working as Director of a CyberSecurity Lab and is Founder of WHID - We Hack In Disguise: a cybersecurity boutique focused on R&D offensive hardware implants and IIoT Security. Luca is also actively involved in InfoSec where his main fields of research are: Radio Networks, Hardware Hacking, Internet of Things, and Physical Security. At the moment, he is focusing his researches on bypassing biometric access control systems, IIoT Security & Forensics, Air-Gapped Environments and IoOT (Internet of Offensive Things).

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 14:00-14:59 PDT

Title: HandPwning: “Your Hand is your Passport. Verify me. Now let me in!”
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Biometrics applied to PACS (Physical Access Control Systems) has been an hot-topic for a few years now. The spread of fingerprint or face recognition based access control and time attendance systems among corporate, industrial and military environments has surged. And with it, also the number of potential attack vectors has increased. In this talk, after a brief overview of the state of art of available PACS utilizing biometrics to authenticate and authorize users, we will investigate one technology among others (usually perceived less-invasive) that has been widely used in some specific fields (e.g. industrial plants, airports, food industry, etc.): the handpunch access control and time attendance systems. The handpunch PACS are based on the hand-geometry recognition. In this presentation we will have a look how this tech works and, in particular, we will focus our attention on reviewing some of existing handpunch devices: from a physical security POV until reversing the communication protocol. Moreover, during the presentation will be demonstrated how to remotely push a new super-admin user into it (i.e. persistent backdoor), how to dump existing users credentials and will be also released an opensource tool-suite: HandScan & HandPwner. Eventually, thanks the cooperation with Shodan’s creator, it has been confirmed that more than 1800 of these vulnerable devices were found exposed on the Internet. Finally, we will conclude the talk with practical and actionable countermeasures to prevent these attacks and how to harden these devices.

SpeakerBio: Luca "CYBERANTANI" Bongiorni, Founder at We Hack In Disguise (WHID)
Luca Bongiorni is working as Director of a CyberSecurity Lab and is Founder of WHID - We Hack In Disguise: a cybersecurity boutique focused on R&D offensive hardware implants and IIoT Security. Luca is also actively involved in InfoSec where his main fields of research are: Radio Networks, Hardware Hacking, Internet of Things, and Physical Security. At the moment, he is focusing his researches on bypassing biometric access control systems, IIoT Security & Forensics, Air-Gapped Environments and IoOT (Internet of Offensive Things).

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 10:00-17:59 PDT

Title: Hands-on Attack and Breach Simulation exercises
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

This area will feature guided breach simulation exercises for participants to engage with. There will be two activities, "Breach-the-Hospital" and "Breach-the-Office," based on two LEGO sets. A simulated cyber range will be available for each scenario, providing an exact replica of an enterprise production environment. We will provide a detailed walkthrough of the attack scenarios, including Tools-Techniques-and-Procedures (TTPs) commands and how-to guides, demonstrating how to atatck and breach the hospital's infrastructure or the office environment. This exercise will give participants a clear understanding of how adversaries infiltrate corporate environments.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Sunday - 10:00-11:59 PDT

Title: Hands-on Attack and Breach Simulation exercises
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

This area will feature guided breach simulation exercises for participants to engage with. There will be two activities, "Breach-the-Hospital" and "Breach-the-Office," based on two LEGO sets. A simulated cyber range will be available for each scenario, providing an exact replica of an enterprise production environment. We will provide a detailed walkthrough of the attack scenarios, including Tools-Techniques-and-Procedures (TTPs) commands and how-to guides, demonstrating how to atatck and breach the hospital's infrastructure or the office environment. This exercise will give participants a clear understanding of how adversaries infiltrate corporate environments.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 10:00-17:59 PDT

Title: Hands-on Attack and Breach Simulation exercises
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV Hands-on Area - Map

Description:

This area will feature guided breach simulation exercises for participants to engage with. There will be two activities, "Breach-the-Hospital" and "Breach-the-Office," based on two LEGO sets. A simulated cyber range will be available for each scenario, providing an exact replica of an enterprise production environment. We will provide a detailed walkthrough of the attack scenarios, including Tools-Techniques-and-Procedures (TTPs) commands and how-to guides, demonstrating how to atatck and breach the hospital's infrastructure or the office environment. This exercise will give participants a clear understanding of how adversaries infiltrate corporate environments.

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 15:40-17:40 PDT

Title: Hands-On Container Image Security: Mastering Sigstore for Unbreachable Integrity
When: Friday, Aug 9, 15:40 - 17:40 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

In the ever-evolving landscape of containerized applications, ensuring the integrity and security of your container images is paramount. Join us for an immersive, hands-on workshop titled "Hands-On Container Image Security: Mastering Sigstore for Unbreachable Integrity," where we'll dive deep into securing your container images using the cutting-edge open-source tools Cosign and Rekor from the Sigstore project.

This workshop will provide a comprehensive, practical introduction to Sigstore tools, demonstrating how they can be seamlessly integrated into your DevOps workflows. We'll begin with a brief overview of the common security challenges associated with container images and how Sigstore addresses these issues by providing automated and tamper-proof signing and verification processes.

Participants will then engage in hands-on exercises, where they'll: 1. Learn to sign container images and verify their integrity using Cosign. We'll guide you through setting up Cosign, signing your first image, and verifying its signature, ensuring you have a solid understanding of this powerful tool. 2. Delve into using Rekor, Sigstore's transparency log, to record and verify signed image metadata. You'll experience firsthand how Rekor enhances security by providing an immutable log of all signed images, ensuring accountability and traceability. 3. Discover how to seamlessly integrate these tools into your existing DevOps pipelines, automating the signing and verification process, and ensuring that only trusted and verified images make it to production environments.

By the end of this workshop, you'll have gained hands-on experience with Sigstore tools and a deep understanding of how to implement them in your own environment. This session is tailored for DevOps engineers, security professionals, and software developers who are committed to enhancing their container security practices.

Don't miss this unique opportunity to acquire practical knowledge and skills in securing your container images. Join us and learn how to leverage Sigstore's powerful tools to ensure your container images are secure, verified, and trustworthy, safeguarding your applications from potential threats.

Speakers:Mohammed Ilyas Ahmed,Syed Aamiruddin

SpeakerBio: Mohammed Ilyas Ahmed

Mohammed Ilyas Ahmed is an industry professional with extensive expertise in security within the DevSecOps domain, where he diligently works to help organizations bolster their security practices. With a fervent dedication to enhancing security posture, Mohammed's insights and guidance are invaluable to those navigating the complex landscape of DevSecOps. In addition to his involvement in industry events, Mohammed is an active speaker and judge, lending his expertise to technical sessions at prestigious conferences. His commitment to advancing knowledge is evident through his research contributions at Harvard University, where he contributes to journal publications, enriching the academic discourse surrounding security practices, and as a distinguished member of the Harvard Business Review Advisory Council, underscores his commitment to advancing knowledge and fostering collaboration between academia and industry. Mohammed Ilyas Ahmed's influence extends even further as a Member of the Global Advisory Board at Vigitrust Limited, based in Dublin, Ireland. This additional role highlights his international reach and his involvement in shaping global strategies for cybersecurity and data protection. Mohammed's dedication to excellence is further highlighted by his numerous certifications, which serve as a testament to his proficiency and depth of knowledge in the security domain. However, beyond his professional pursuits, Mohammed is a multifaceted individual with a diverse range of interests, adding richness to his character and perspective.

SpeakerBio: Syed Aamiruddin

Aamiruddin Syed is a Senior Product Security Engineer with over eight years of industry experience. Specializing in DevSecOps, Shift-Left Security, cloud security, and internal penetration testing, he excels in automating security within CI/CD pipelines, developing security automation, and integrating security into infrastructure as code. His work involves securing cloud platforms by implementing best infrastructure provisioning and configuration practices. His penetration testing skills enable him to conduct targeted internal assessments of critical applications and systems, proactively identifying risks. He bridges the gap between security and engineering teams, embedding security directly into products, including those in the manufacturing sector. Aamiruddin holds dual master's degrees in Cybersecurity from Northeastern University and Jadavpur University. As a recognized security advocate, he frequently speaks at industry conferences, chairs technical conferences such as ICCTICT, and serves as a judge for the Globee Awards for Cybersecurity. He actively contributes to open-source security tools designed to make security seamless for developers. In his free time, Aamiruddin enjoys traveling and photography.

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Rapid7 is back with more hands-on hardware hacking exercises. This year we will be guiding attendees through several exercises gaining root access for control and extraction of firmware and file system data. From TFTP kernel images over the network to single user mode access via modification of U-Boot. These exercises will guide you through the process of importing a kernel image over the network and executing it in memory for root access, along with understanding embedded device flash memory layout and how to transfer firmware images over the network for offline testing.“ Also, we will walk through placing the IoT device in single user mode for root access and then rebuild the structure and needed drivers to bring the IoT embedded system out of single user mode for full access.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Rapid7 is back with more hands-on hardware hacking exercises. This year we will be guiding attendees through several exercises gaining root access for control and extraction of firmware and file system data. From TFTP kernel images over the network to single user mode access via modification of U-Boot. These exercises will guide you through the process of importing a kernel image over the network and executing it in memory for root access, along with understanding embedded device flash memory layout and how to transfer firmware images over the network for offline testing.“ Also, we will walk through placing the IoT device in single user mode for root access and then rebuild the structure and needed drivers to bring the IoT embedded system out of single user mode for full access.

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Rapid7 is back with more hands-on hardware hacking exercises. This year we will be guiding attendees through several exercises gaining root access for control and extraction of firmware and file system data. From TFTP kernel images over the network to single user mode access via modification of U-Boot. These exercises will guide you through the process of importing a kernel image over the network and executing it in memory for root access, along with understanding embedded device flash memory layout and how to transfer firmware images over the network for offline testing.“ Also, we will walk through placing the IoT device in single user mode for root access and then rebuild the structure and needed drivers to bring the IoT embedded system out of single user mode for full access.

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 12:00-13:59 PDT

Title: Hands-on Kubernetes security with KubeHound (purple teaming)
When: Saturday, Aug 10, 12:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

There’s no two ways about it: Kubernetes is a confusing and complex collection of intertwined systems. Finding attack paths in Kubernetes by hand is a frustrating, slow, and tedious process. Defending Kubernetes against those same attack paths is almost impossible without any third party tooling. In this workshop we will present KubeHound - an opinionated, scalable, offensive-minded Kubernetes attack graph tool used by security teams across Datadog. We will cover the custom KubeHound DSL to demonstrate its power to identify some of the most interesting and common attack primitives living in your Kubernetes cluster. If the DSL is not enough, we will cover the basics of Gremlin, the language used by our graph technology so you can find relevant attack paths that matter to you. As attackers (or defenders), there's nothing better to understand an attack than to exploit it oneself. So in this workshop we will cover some of the usual attack paths and exploit them.

SpeakerBio: Julien Terriac, Adversary Simulation Engineering at Datadog

Julien Terriac a French senior security researcher with a strong background of pentesting with a special taste for Windows authentication, Active Directory inner working and reverse engineering. He developed several offensive tools to automate such as ProtonPack (custom mimikatz), Lycos (share hunter), ExploitPack (privilege escalation framework), IAMBuster (AD auditing framework).He led the R&D department at XMCO for 5 years before joining Datadog as the Team Lead for Adversary Simulation Engineering (ASE) where his team aims at building offensive tools and frameworks that will automate the simulation of real life attacks against Datadog.

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 15:00-16:59 PDT

Title: Hands-on workshop
When: Friday, Aug 9, 15:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Hard Hat Brigade - Community Space Open
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-02 - Map

Description:

Ever see someone walking around DEF CON and wonder “what is up with the hard hats?”

The Hard Hat Brigade brings hackers together in the spirit of endless curiosity and tinkering. We use a common platform (hats) to combine art (bling) and hacker functionality (warez) to inspire others to explore outside of their comfort zones in a safe and welcoming community.

We encourage everyone to explore their creativity using art, electronics, mechanical design, or any other medium that piques their interest. Hats are inexpensive, widely available, and easy to modify to suit your needs. We started with hard hats but are not limited to any type of hat, so you have the freedom to choose whatever hat suits your fancy.

Despite everyone using a common platform, every creation is unique and embodies the personality of the creator. Walking around DEF CON, you can display your creation for all to see, and many will stop to ask you about what you have created. This allows you to talk about your experience, as well as inspire others to explore new ideas of their own.

One of the challenges at hacker summer camp has been finding people to connect with. By leveraging hard hats as a canvas, HHB has solved this challenge with something that is incredibly accessible while also offering a ton of variety. Gazing upon these creations, they reflect back the uniqueness of all the awesome hackers that we’ve been able to meet. In years past, we’ve had the opportunity to see how so many talented and creative hackers tackle the challenge of using the venerable hard hat as their muse. Just as fun, charming and skilled as so many attendees are, the hard hat has been a great vessel to carry their awesome projects.

Stop by our community space and make your trip memorable by trying on a hat, learning and sharing building techniques, networking with other hat loving hackers, and expressing yourself in your own hacker way. Keep on hacking!

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Hard Hat Brigade - Community Space Open
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-02 - Map

Description:

Ever see someone walking around DEF CON and wonder “what is up with the hard hats?”

The Hard Hat Brigade brings hackers together in the spirit of endless curiosity and tinkering. We use a common platform (hats) to combine art (bling) and hacker functionality (warez) to inspire others to explore outside of their comfort zones in a safe and welcoming community.

We encourage everyone to explore their creativity using art, electronics, mechanical design, or any other medium that piques their interest. Hats are inexpensive, widely available, and easy to modify to suit your needs. We started with hard hats but are not limited to any type of hat, so you have the freedom to choose whatever hat suits your fancy.

Despite everyone using a common platform, every creation is unique and embodies the personality of the creator. Walking around DEF CON, you can display your creation for all to see, and many will stop to ask you about what you have created. This allows you to talk about your experience, as well as inspire others to explore new ideas of their own.

One of the challenges at hacker summer camp has been finding people to connect with. By leveraging hard hats as a canvas, HHB has solved this challenge with something that is incredibly accessible while also offering a ton of variety. Gazing upon these creations, they reflect back the uniqueness of all the awesome hackers that we’ve been able to meet. In years past, we’ve had the opportunity to see how so many talented and creative hackers tackle the challenge of using the venerable hard hat as their muse. Just as fun, charming and skilled as so many attendees are, the hard hat has been a great vessel to carry their awesome projects.

Stop by our community space and make your trip memorable by trying on a hat, learning and sharing building techniques, networking with other hat loving hackers, and expressing yourself in your own hacker way. Keep on hacking!

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Hard Hat Brigade - Community Space Open
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-02 - Map

Description:

Ever see someone walking around DEF CON and wonder “what is up with the hard hats?”

The Hard Hat Brigade brings hackers together in the spirit of endless curiosity and tinkering. We use a common platform (hats) to combine art (bling) and hacker functionality (warez) to inspire others to explore outside of their comfort zones in a safe and welcoming community.

We encourage everyone to explore their creativity using art, electronics, mechanical design, or any other medium that piques their interest. Hats are inexpensive, widely available, and easy to modify to suit your needs. We started with hard hats but are not limited to any type of hat, so you have the freedom to choose whatever hat suits your fancy.

Despite everyone using a common platform, every creation is unique and embodies the personality of the creator. Walking around DEF CON, you can display your creation for all to see, and many will stop to ask you about what you have created. This allows you to talk about your experience, as well as inspire others to explore new ideas of their own.

One of the challenges at hacker summer camp has been finding people to connect with. By leveraging hard hats as a canvas, HHB has solved this challenge with something that is incredibly accessible while also offering a ton of variety. Gazing upon these creations, they reflect back the uniqueness of all the awesome hackers that we’ve been able to meet. In years past, we’ve had the opportunity to see how so many talented and creative hackers tackle the challenge of using the venerable hard hat as their muse. Just as fun, charming and skilled as so many attendees are, the hard hat has been a great vessel to carry their awesome projects.

Stop by our community space and make your trip memorable by trying on a hat, learning and sharing building techniques, networking with other hat loving hackers, and expressing yourself in your own hacker way. Keep on hacking!

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 12:00-12:59 PDT

Title: Hard Hat Brigade - Group Photo and People's Choice Award
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-02 - Map

Description:

Join us for our annual group photo and voting session for the "People's Choice Award". Even though we don't have a contest, as a community we can still choose a favorite hat. We have to take the picture at 12:05 sharp so be there!

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 14:00-14:59 PDT

Title: Hard Hat Brigade - Q&A Panel
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-02 - Map

Description:

Get all your questions about hard hats answered by the Hard Hat Brigade community organizers.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 14:00-14:59 PDT

Title: Hard Hat Brigade Maker Panel
When: Friday, Aug 9, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-02 - Map

Description:

Ask other hard hat enthusiasts about tips, tricks, and techniques during the Hard Hat Makers Panel. Power? Bling? Warez? Process? Let us help you on your own build journey.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Hardware Hacking and Soldering Skills Village Open (HHV-SSV)
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Hardware Hacking and Soldering Skills Village Open (HHV-SSV)
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Hardware Hacking and Soldering Skills Village Open (HHV-SSV)
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Hardware Hacking GE Appliances
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

How to get started, two steps

```
Download the GE Appliances SmartHQ App “SmartHQ” available on the Google Play and iOS Stores to your
Create your GE Appliances Account to commission the appliance, connecting the appliance to your acco
```

Router Name SSID: HackAway Router Name Password: With GEA

In-Scope: Only communications between the appliance, GE Appliances SmartHQ App, and the cloud connection for the appliance

Please leave your contact information and we will be in touch! Or you may visit our security webpage by typing “GEAppliances.com/security” into your Internet browser. We have a call center and PSIRT team ready to hear your questions!

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Hardware Hacking GE Appliances
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

How to get started, two steps

```
Download the GE Appliances SmartHQ App “SmartHQ” available on the Google Play and iOS Stores to your
Create your GE Appliances Account to commission the appliance, connecting the appliance to your acco
```

Router Name SSID: HackAway Router Name Password: With GEA

In-Scope: Only communications between the appliance, GE Appliances SmartHQ App, and the cloud connection for the appliance

Please leave your contact information and we will be in touch! Or you may visit our security webpage by typing “GEAppliances.com/security” into your Internet browser. We have a call center and PSIRT team ready to hear your questions!

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Hardware Hacking GE Appliances
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

How to get started, two steps

```
Download the GE Appliances SmartHQ App “SmartHQ” available on the Google Play and iOS Stores to your
Create your GE Appliances Account to commission the appliance, connecting the appliance to your acco
```

Router Name SSID: HackAway Router Name Password: With GEA

In-Scope: Only communications between the appliance, GE Appliances SmartHQ App, and the cloud connection for the appliance

Please leave your contact information and we will be in touch! Or you may visit our security webpage by typing “GEAppliances.com/security” into your Internet browser. We have a call center and PSIRT team ready to hear your questions!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Hardware Hacking Village CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

Grab some solder and update your JTAGulator! The Hardware Hacking Village (HHV) is back with another DEF CON hardware hacking-focused Capture the Flag (CTF) competition. This is a jeopardy style CTF, designed to challenge participants in various aspects of hardware hacking. Whether you're new to hardware hacking or experienced and just looking for something to do while you wait for your fault injection to trigger, all are welcome and challenges range from beginner to advanced.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Hardware Hacking Village CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

Grab some solder and update your JTAGulator! The Hardware Hacking Village (HHV) is back with another DEF CON hardware hacking-focused Capture the Flag (CTF) competition. This is a jeopardy style CTF, designed to challenge participants in various aspects of hardware hacking. Whether you're new to hardware hacking or experienced and just looking for something to do while you wait for your fault injection to trigger, all are welcome and challenges range from beginner to advanced.

Return to Index - Add to Google - ics Calendar file

ESV - Saturday - 10:00-17:59 PDT

Title: Hardware Hacking: Glitching Lab
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Curious about hacking chips using fault-injection? Take your first steps in our (free) glitching workshops! We provide you with hardware & guidance to conduct your first fault-injection attacks, all you need is a laptop running Python & OpenOCD: Reproduce the nRF52 "AirTag" glitch or learn how to glitch one of the chips used in crypto-wallets to store millions of dollars.

We will also have a secret challenge announced on site!

Lab provided by hextree.io

Return to Index - Add to Google - ics Calendar file

ESV - Friday - 10:00-17:59 PDT

Title: Hardware Hacking: Glitching Lab
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Curious about hacking chips using fault-injection? Take your first steps in our (free) glitching workshops! We provide you with hardware & guidance to conduct your first fault-injection attacks, all you need is a laptop running Python & OpenOCD: Reproduce the nRF52 "AirTag" glitch or learn how to glitch one of the chips used in crypto-wallets to store millions of dollars.

We will also have a secret challenge announced on site!

Lab provided by hextree.io

Return to Index - Add to Google - ics Calendar file

ESV - Sunday - 10:00-12:59 PDT

Title: Hardware Hacking: Glitching Lab
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Curious about hacking chips using fault-injection? Take your first steps in our (free) glitching workshops! We provide you with hardware & guidance to conduct your first fault-injection attacks, all you need is a laptop running Python & OpenOCD: Reproduce the nRF52 "AirTag" glitch or learn how to glitch one of the chips used in crypto-wallets to store millions of dollars.

We will also have a secret challenge announced on site!

Lab provided by hextree.io

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: HardWired
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

This event was born out of the desire to teach an often-overlooked hardware and networking skill, and to provide the opportunity for experienced people to mentor others as they learn. DEF CON provides the perfect environment for people with no prior training to learn something useful and new. Hardwired networks are often overlooked in today's world of cellular connection and Wi-Fi, but they still play an important part in the backbone of information sharing. We believe that while cutting-edge technologies are thrilling, traditional skills-building still has its place, and we want to provide that opportunity to the DEF CON community.

Don't know how to make a network cable and want to learn? Has it been years? Or do you think you're a pro? Come see if you can... make the best cable at con by cut/wire/crimp.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: HardWired
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

This event was born out of the desire to teach an often-overlooked hardware and networking skill, and to provide the opportunity for experienced people to mentor others as they learn. DEF CON provides the perfect environment for people with no prior training to learn something useful and new. Hardwired networks are often overlooked in today's world of cellular connection and Wi-Fi, but they still play an important part in the backbone of information sharing. We believe that while cutting-edge technologies are thrilling, traditional skills-building still has its place, and we want to provide that opportunity to the DEF CON community.

Don't know how to make a network cable and want to learn? Has it been years? Or do you think you're a pro? Come see if you can... make the best cable at con by cut/wire/crimp.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: HardWired
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

This event was born out of the desire to teach an often-overlooked hardware and networking skill, and to provide the opportunity for experienced people to mentor others as they learn. DEF CON provides the perfect environment for people with no prior training to learn something useful and new. Hardwired networks are often overlooked in today's world of cellular connection and Wi-Fi, but they still play an important part in the backbone of information sharing. We believe that while cutting-edge technologies are thrilling, traditional skills-building still has its place, and we want to provide that opportunity to the DEF CON community.

Don't know how to make a network cable and want to learn? Has it been years? Or do you think you're a pro? Come see if you can... make the best cable at con by cut/wire/crimp.

Return to Index - Add to Google - ics Calendar file

HDA - Friday - 18:00-23:59 PDT

Title: HDA Chillout w/ Dj Delchi
When: Friday, Aug 9, 18:00 - 23:59 PDT
Where: LVCC West/Floor 1/W110 - Map

Description:

Chillout to etherial / downtempo tunes and hang with your community

Return to Index - Add to Google - ics Calendar file

HDA - Saturday - 10:00-23:59 PDT

Title: HDA Community - Open for Accessibility Questions/Help
When: Saturday, Aug 10, 10:00 - 23:59 PDT
Where: LVCC West/Floor 1/W110 - Map

Description:

DEF CON has made HDA a community, and we now have a community room! This room will be dedicated to the attendees with ADA needs, their friends, helpers, and anyone who wants to hang out and be social! So far we plan on providing charging stations, chill out sessions, an open call for a modular synth jam session, and more to come! Let's all work together to make DEFCON Awesomely Accessible!

(Please note that on Thursday, we will be open only to provide assistance to those in need. Regular community programming will begin on Friday.)

Hang out, chill out deck out your mobility device and more!

Return to Index - Add to Google - ics Calendar file

HDA - Friday - 10:00-23:59 PDT

Title: HDA Community - Open for Accessibility Questions/Help
When: Friday, Aug 9, 10:00 - 23:59 PDT
Where: LVCC West/Floor 1/W110 - Map

Description:

DEF CON has made HDA a community, and we now have a community room! This room will be dedicated to the attendees with ADA needs, their friends, helpers, and anyone who wants to hang out and be social! So far we plan on providing charging stations, chill out sessions, an open call for a modular synth jam session, and more to come! Let's all work together to make DEFCON Awesomely Accessible!

(Please note that on Thursday, we will be open only to provide assistance to those in need. Regular community programming will begin on Friday.)

Hang out, chill out deck out your mobility device and more!

Return to Index - Add to Google - ics Calendar file

HDA - Sunday - 10:00-14:59 PDT

Title: HDA Community - Open for Accessibility Questions/Help
When: Sunday, Aug 11, 10:00 - 14:59 PDT
Where: LVCC West/Floor 1/W110 - Map

Description:

DEF CON has made HDA a community, and we now have a community room! This room will be dedicated to the attendees with ADA needs, their friends, helpers, and anyone who wants to hang out and be social! So far we plan on providing charging stations, chill out sessions, an open call for a modular synth jam session, and more to come! Let's all work together to make DEFCON Awesomely Accessible!

(Please note that on Thursday, we will be open only to provide assistance to those in need. Regular community programming will begin on Friday.)

Hang out, chill out deck out your mobility device and more!

Return to Index - Add to Google - ics Calendar file

HDA - Thursday - 10:00-17:59 PDT

Title: HDA Community - Open for Accessibility Questions/Help
When: Thursday, Aug 8, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/W110 - Map

Description:

DEF CON has made HDA a community, and we now have a community room! This room will be dedicated to the attendees with ADA needs, their friends, helpers, and anyone who wants to hang out and be social! So far we plan on providing charging stations, chill out sessions, an open call for a modular synth jam session, and more to come! Let's all work together to make DEFCON Awesomely Accessible!

(Please note that on Thursday, we will be open only to provide assistance to those in need. Regular community programming will begin on Friday.)

Hang out, chill out deck out your mobility device and more!

Return to Index - Add to Google - ics Calendar file

HDA - Friday - 14:00-15:59 PDT

Title: HDA Presents : Naomi Brockwell
When: Friday, Aug 9, 14:00 - 15:59 PDT
Where: LVCC West/Floor 1/W110 - Map

Description:

Talk on health info privacy

SpeakerBio: Naomi Brockwell, NBTV
No BIO available

Return to Index - Add to Google - ics Calendar file

HDA - Saturday - 12:00-15:59 PDT

Title: HDA Presents the open Synth Jam Session
When: Saturday, Aug 10, 12:00 - 15:59 PDT
Where: LVCC West/Floor 1/W110 - Map

Description:

Bring your instruments, synths, and self for an open jam session

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: HHV Rube Goldberg Machine
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

To celebrate DEF CON 32, the Hardware Hacking Village (HHV) is hosting a Rube Goldberg Machine (RGM) Event! This idea has been kicking around the HHV volunteer circle in one shape or another since at least DEF CON 20, so it's about time that it happened! The goal is to create a series of devices that combine to form an end-to-end Rube Goldberg machine for transmitting messages. The hope is that all sorts of creative devices will be connected up to each other to move bits through various complicated and fun analog/digital methods. Ideas have ranged from simply wiring RX to TX — to using radios to bounce the message off the moon!

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: HHV Rube Goldberg Machine
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

To celebrate DEF CON 32, the Hardware Hacking Village (HHV) is hosting a Rube Goldberg Machine (RGM) Event! This idea has been kicking around the HHV volunteer circle in one shape or another since at least DEF CON 20, so it's about time that it happened! The goal is to create a series of devices that combine to form an end-to-end Rube Goldberg machine for transmitting messages. The hope is that all sorts of creative devices will be connected up to each other to move bits through various complicated and fun analog/digital methods. Ideas have ranged from simply wiring RX to TX — to using radios to bounce the message off the moon!

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: HHV Rube Goldberg Machine
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

To celebrate DEF CON 32, the Hardware Hacking Village (HHV) is hosting a Rube Goldberg Machine (RGM) Event! This idea has been kicking around the HHV volunteer circle in one shape or another since at least DEF CON 20, so it's about time that it happened! The goal is to create a series of devices that combine to form an end-to-end Rube Goldberg machine for transmitting messages. The hope is that all sorts of creative devices will be connected up to each other to move bits through various complicated and fun analog/digital methods. Ideas have ranged from simply wiring RX to TX — to using radios to bounce the message off the moon!

Return to Index - Add to Google - ics Calendar file

DL - Friday - 14:00-15:45 PDT

Title: HIDe & SEEK
When: Friday, Aug 9, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W304 - Map

Description:

The Injectyll-HIDe project (released at DEF CON 30) is back and better than ever! The hardware implant utilizes the same standard features that you have come to know and love (keystroke recording, keystroke injection, mouse jiggler, etc.) but it has evolved into so much more. The functionality has been steadily growing over its initial release to offer users even more tools! But wait, there's more! We're proud to show off the new SEEK shields this year at the CON! Tired of running a covert mesh network? Want to try out new RF technologies? We've added LoRa and LoRaWAN to the mix as well! These shields are field swappable and work with the existing C2 and implant code to give you the versatility that you need to continue evading detection. Attendees should be prepared to flip 0ut over these features, as well as some new additions to the project that we will be announcing at DEF CON. Who's ready for a high stakes game of hacker's HIDe and SEEK?

Speakers: Jonathan Fischer,Matthew Richard

SpeakerBio: Jonathan Fischer, Red Team Consultant and Researcher

Jonathan Fischer (a.k.a. c4m0ufl4g3) is a hardware and IoT security enthusiast that started off designing, programming, and implementing electronic controls for industrial control systems and off-highway machinery. After a decade in that industry, Jonathan obtained his BS in Computer Science and transitioned over to the cyber security industry where he has been working as a Red Team consultant and researcher for more than seven years at a Fortune 500 company. Since joining the cyber security industry, Jonathan has earned various industry certifications (OSCP, GXPN, etc.) and continues to leverage his unique experience in his research into hardware hacking. Jonathan has presented his research at conferences such as DEF CON Demo Labs, ShmooCon, THOTCON, BSides LV, and Hardware Hacking Village. He is also the co-creator of Injectyll-HIDe, an open-source hardware implant designed for use by red teams.

SpeakerBio: Matthew Richard

Matthew Richard is a software developer that enjoys coding in low level languages. His favorite text editor is Neovim. As an average Neovim enjoyer he is obligated to stand on the side of Vi in the text editor war, but chooses to be on the side of Ed to make everyone equally unhappy. His operating system of choice is NixOS... by the way. :)

Return to Index - Add to Google - ics Calendar file

Title: High Intensity Deconstruction: Chronicles of a Cryptographic Heist
When: Friday, Aug 9, 11:30 - 12:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Introduced in 2011, HID Global's iCLASS SE solution is one of the world's most widely-deployed Electronic Physical Access Control platforms. HID's iCLASS SE Readers are ubiquitous in electronic physical access control and used in most government agencies and Fortune 500 companies. The readers can be easily seen and identified in almost every form of mainstream media. Almost 13 years after iCLASS SE's introduction, ground-breaking research and technical exploits will be disclosed publicly for the first time.

In this talk, we detail the process by which we reverse engineered the complex hardware and software chain of trust securing HID's iCLASS SE platform.

Over a seven-year research period, we analyzed hardware, firmware, and software elements the ecosystem, uncovering an unfortunate series of pitfalls and implementation defects. These flaws culminated in an attack chain that allowed for the recovery of sensitive cryptographic key material from secure elements, which have received CC EAL 5+ accreditation. This chain resulted in revealing some cryptographic keys to the kingdom.

Finally, we provide comprehensive guidance on technical and operational mitigations for end customers to identify practical risks and reduce impact.

Inspirational (research done on previous generation system)

- Heart of Darkness - Milosch Meriac link
- Dismantling iClass and iClass Elite - Garcia, de Koning Gans, Verdult, & Meriac link

Speakers: Babak Javadi,Aaron Levy,Nick Draffen

SpeakerBio: Babak Javadi, Founder at The CORE Group

Babak Javadi is the Founder of The CORE Group and Co-Founder of the Red Team Alliance, a covert entry training and certification body. As a professional red teamer with over a decade of field experience, Babak's expertise includes a wide range of disciplines, from high security mechanical cylinders to alarm systems and physical access control platforms. Babak's community contributions include the co-founding of The Open Organisation of Lockpickers (TOOOL) where he served on the Board of Directors for over 13 years.

SpeakerBio: Aaron Levy, Lead of Security Engineering at Clover

Aaron Levy is an independent security researcher that was credited in the discovery of CVE-2018-10897 and CVE-2019-11630. In his day job, he leads Security Engineering for Clover, a Payments and Point of Sale company that is a subsidiary of Fiserv.

SpeakerBio: Nick Draffen, Product Security Architect

Nick Draffen is a Product Security Architect, focusing on the protection of laboratory instruments and their software. Outside of work, he dives into research, reverse engineering, and hardware hacking, leveraging his technical expertise to both build and break things. He is a member of the Security Tribe and volunteers with the RF Village, creating and overseeing challenges for the RF CTF at various security conferences. Always eager to lend a helping hand, he is known for his ability to pull just

the right tool from his extensive bag of tricks.

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 14:30-15:59 PDT

Title: High ROI Manual Bug Hunting Techniques
When: Saturday, Aug 10, 14:30 - 15:59 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

Who isn't busy nowadays? When you sit down to hack, you want to find a bug, or at least know you're on the right track to find one. Over the past 5 years of full-time bug bounty, I've identified a couple of techniques that will get you some quick wins on most applications. I'll show you how to apply these techniques, and then, building upon them, direct your longer-term testing to keep finding bugs and getting the best ROI for your time hunting. This workshop is oriented toward equipping you to make the most money with the least time investment. These are not the most technical bugs. These are the bugs that pay the bills and keep you well-fed, dopamine'ed up, and pushing deeper into these apps. In this workshop, we'll target REAL bug bounty targets, and apply the very techniques I've used in the past to find bugs on these targets. We'll cover mega-efficient testing techniques for various types of client-side access controls and IDORs. We'll cover polyglot usage for generic injection testing. We'll cover attack vector ideation, friction minimization, gadget hunting, organization. And much, much more. All of these things will keep you motivated, on track, and efficient as you push through the slog of HTTP requests between you and your next pay day. Leggo.

What skill level is your presentation aimed at? All skill levels, but attendees should have a basic understanding of web architecture and web vulnerabilities such as XSS, CSRF, IDOR, and Broken Access Controls.

Pre-Requisites: - Bring your laptop - Please come with Caido installed (or Burp, if you must) - General understanding of HTTP requests and web testing

SpeakerBio: Justin "Rhynorater" Gardner, Host at Critical Thinking - Bug Bounty Podcast

Yo! I'm Justin Gardner - a full-time bug bounty hunter out of Richmond, VA. I also host the Critical Thinking - Bug Bounty Podcast and advise for Caido - the latest and greatest HTTP proxy.

I'm an active member of the HackerOne live hacking event circuit (the medium through which I do most of my bug bounties) and have placed top 5 in most of the live hacking events I've attended for the past couple years. Web hacking is my sh*t, but I love all types of hacking.

Outside of hacking, I love volleyball, I love Jesus, and I love startups. Those, with a healthy dose of family and friends, keep all my free time on lock.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 15:30-16:15 PDT

Title: HookChain: A new perspective for Bypassing EDR Solutions
When: Saturday, Aug 10, 15:30 - 16:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

In the current digital security ecosystem, where threats evolve rapidly and with complexity, companies developing Endpoint Detection and Response (EDR) solutions are in constant search for innovations that not only keep up but also anticipate emerging attack vectors. In this context, this article introduces the HookChain, a look from another perspective at widely known techniques, which when combined, provide an additional layer of sophisticated evasion against traditional EDR systems.

Through a precise combination of IAT Hooking techniques, dynamic SSN resolution, and indirect system calls, HookChain redirects the execution flow of Windows subsystems in a way that remains invisible to the vigilant eyes of EDRs that only act on Ntdll.dll, without requiring changes to the source code of the applications and malwares involved.

This work not only challenges current conventions in cybersecurity but also sheds light on a promising path for future protection strategies, leveraging the understanding that continuous evolution is key to the effectiveness of digital security.

By developing and exploring the HookChain technique, this study significantly contributes to the body of knowledge in endpoint security, stimulating the development of more robust and adaptive solutions that can effectively address the ever-changing dynamics of digital threats. This work aspires to inspire deep reflection and advancement in the research and development of security technologies that are always several steps ahead of adversaries.

SpeakerBio: Helvio Carvalho Junior, CEO at Sec4US

Helvio is the CEO of Sec4US, a leading company in Cyber Security, and stands out as a renowned researcher in the field. He made history by being the first in Latin America to achieve the prestigious OSCE3 certification, a milestone that reflects his deep knowledge and technical skill. With over 23 years of experience across various segments of Information Technology, Helvio currently focuses on research in bypass techniques for Endpoint Detection and Antivirus solutions, as well as specializing in offensive information security (RedTeam). His passion for creating exploits and malware is well-known and significantly contributes to the advancement of cybersecurity.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 14:00-15:45 PDT

Title: Hopper - Distributed Fuzzer
When: Friday, Aug 9, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W308 - Map

Description:

Hopper is a Coverage-Guided Greybox Distributed Fuzzer, inspired by AFL++, and written in Golang. Like other fuzzers, Hopper operates as a standard command-line interface tool, allowing you to run fuzz campaigns to find vulnerabilities and exploits in software. Hopper's mutation algorithm, energy assigning strategy, and out-of-process coverage gathering, are all inspired by AFL++, the current state of the art fuzzer. However, Hopper's distributed strategy differs substantially than AFL++ in an attempt to define a new distributed fuzzing paradigm. AFL++ and LibFuzzer have clear scaling limitations in larger environments, notably the AFL++'s rudimentary multi-machine mode. As an early prototype, Hopper addresses these limitations by implementing a deduplicating communication schema that establishes a consistency invariant, minimizing repeated work done by fuzzing nodes. Hopper is a standalone, new piece of software developed from scratch in the spirit of exploration, this is not yet another python plugin/extension for AFL++. Hopper is currently available on GitHub, including containerized runnable campaign demos. Tooling and observability are first class features, in the form of a TUI to monitor fuzzing campaigns, usage docs, and quick-start scripts for orchestrating fuzz campaigns.

Speakers: Luciano Remes,Wade Cappa

SpeakerBio: Luciano Remes, Software Engineer at Palantir Technologies

Luciano Remes received a B.S. in Computer Science from the University of Utah, where he did 2 years of grant-funded Systems research under the FLUX Research Group, finally working on his Thesis Hopper: Distributed Fuzzer. During this time, he also interned at AWS EC2 and Goldman Sachs SPARC infrastructure teams, as well as a few startups including Blerp and Basecamp. Currently, he's a Software Engineer at Palantir Technologies building distributed network infrastructure.

SpeakerBio: Wade Cappa, Software Engineer at Palantir Technologies

Wade Cappa recently graduated from Washington State University with a B.S in Computer Science and is now working at Palantir Technologies as a Software Engineer on distributed data systems. He previously worked at Microsoft in the Semantic Machines department, creating a dynamically linked debugging utility for an internal use tooling language. In his freetime he is working with a high-performance-computing research group on a cutting edge distributed strategy for approximating submodular monotonic optimizations.

Return to Index - Add to Google - ics Calendar file

Title: Hospitals, Airports, and Telcos — Modern Approach to Attributing Hacktivism Attacks
When: Friday, Aug 9, 11:30 - 12:05 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

On December 12th, millions of Ukrainians trying to connect on Kyivstar's mobile and internet services were met with silence. The outage, it turned out, was no accident, but a carefully planned attack that had been brewing for months. One day later, a message saying “We take full responsibility for the cyber attack on Kyivstar” appeared on social media accounts belonging to a group calling itself ‘Solntsepek’.

“We attacked Kyivstar because the company provides communications to the Armed Forces of Ukraine” the message continued. The Ukrainian users found themselves an audience of another hacking stunt in the ongoing war that started with the Russian invasion of Ukraine. Almost one month later, the pro-Ukraine hacker group “BlackJack” claimed to have breached the Russian internet provider M9com as revenge for the Kyivstar attack.

These attacks demonstrate a rising trend where groups, ostensibly state-sponsored yet posing as hacktivists, execute cyber and influence operations. This approach provides plausible deniability and an appearance of legitimacy, avoiding the direct implications of government involvement. These actors, often using various group names, leverage grassroots facades for anonymity and to minimize international backlash.

But what if the inflation in the trend is its weakest point? This is where yet another trendy topic comes in handy— Machine Learning (And yes, AI as well). We analyzed thousands of public messages from Hacktivist groups in Europe and the Middle East and combined classic Cyber threat-intelligence practices with modern ML models to learn about their motives over time and more importantly — tie some of these groups together and improve the way we do attribution when it comes to Hacktivism.

SpeakerBio: Itay Cohen

No BIO available

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 15:00-15:59 PDT

Title: Hot SOC Topics for 2024: Feel the Spice!
When: Saturday, Aug 10, 15:00 - 15:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

This panel is a reprisal of the panel I've done for a couple years now. The first two years we were very successful- packed room, high audience engagement. I'm hoping to come back for a third year.

This is not written for public consumption. If you want a longer description that's audience-facing, let me know!

* Topic 1- SOCs vs IT infrastructure / Network Ops, the battle continues • Start off by giving some good war stories when we see these groups collide • Then tell some stories where they worked together in success • What is the intended design: efficiency, collaboration, oversight, secrecy? • What techniques makes these relationships successful? • Operational models • Ticketing and tasking • Partnership and interfaces

* Topic 2- LLMs/ Generative AI in general • What are they actually being used for in practice so far • What do we see emerging from the market right now • What roles can we replace in the SOC / adjust staffing on • Let's speculate on 3 years from now, what do we see showing actual value • What's overhyped, so far • Is the SOC going away? (of course it isn't– why not) • Expand scope… what ML techniques outside LLM do we see SOCs getting value out of? What's not getting the attention that it should? • How could we accomplish supervised learning (known / labelled sets) at enough scale? A community driven project might accomplish this. • Unsupervised learning approach - could we accomplish threat intelligence attribution where there's no right answer, but some pretty good basis, and keep refactoring on old campaigns until we have a pretty reasonable approximation? Which leads us to threat intel…

* Topic 3- Threat Intel • Everyone's got feelings about this one, what do we mean by threat intel beyond simple IOC matching? • How much refinement is needed in threat intel reporting? • How are folks separating (and handling) Tactical vs Strategic threat intel? • Who are SOCs getting the most traction with by sharing? Execs? Constituents? Other SOCs? • Work products: • Executive facing reporting? (are execs understanding/getting the value out of these reports?) • IT briefings? • Threat intel production / extraction from investigations? • Attribution?

* Topic 4- Live audience participation • Let's do some live polls of the audience– this worked well last time, let's expand on that • Topics we're considering: • Staffing models • Current hiring trends • Current detection efforts

* Topic 5- Cyber risk quantification • What do we mean by CRQ? • When incidents happen, what CRQ measurement methods actually work? • How are folks using CRQ to drive improvements in defensive controls and/or other risk-related initiatives? • What is more speculative, low value, hard, or otherwise should the audience stay away from?

Come hear 5 SOC veterans discuss some of the most challenging topics in security operations today. Carson Zimmerman is joined by SOC veterans Chris Crowley, Eric Lippart, Enoch Long, and Russ McRee. With a total of over a century of SOC experience, we cut the buzzword bingo and get real. This year, we'll be discussing topics like: resolving conflict with network and IT ops, what value are people really getting out of LLMs, how to get value with threat intel beyond IOC matching, and more! We will be doing live, real-time polling of the audience. We will also take your spicy questions!

Speakers:
Carson Zimmerman,Russ McRee,Eric Lippart,Enoch Long

SpeakerBio:
Carson Zimmerman

Carson Zimmerman has been working in and around security operations centers (SOCs) for over 20 years. In his current role at Ardalyst, Carson helps clients transform uncertainty into understanding in their digital landscape. In his previous role at Microsoft, Carson led the investigations team responsible for defending the M365 platform and ecosystem. His experiences as

a SOC analyst, engineer, and architect led Carson to author Ten Strategies of a World-Class Cybersecurity Operations Center, and co-authored its second edition, Eleven Strategies… which may be downloaded for free at mitre.org/11Strategies.

SpeakerBio: Russ McRee
No BIO available
SpeakerBio: Eric Lippart
No BIO available
SpeakerBio: Enoch Long
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: How can hackers support efforts to secure AI systems?
When: Saturday, Aug 10, 11:00 - 12:20 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

Artificial Intelligence is increasingly being framed in dystopian ways even though the technology has been around for decades and the opportunities it brings are vast. In the past months, more Governments have announced proposals to make AI models and systems more secure. Through a panel session, we want to shine a light on these efforts, particularly those that are most relevant to the DEFCON community, such as recommendations on testing and red teaming as well as the need for vulnerability disclosure processes. This session aims to foster a better understanding of what hackers are seeing on the ground in terms of the vulnerabilities in AI models and to identify how more collaboration could be undertaken. The outcome of this session will be to provide a spotlight on data gaps in this area and to share insights that can positively inform future work, such as the development of international AI standards.

Speakers: Wan Ding Yao,Christine Lai,Anjuli Shere

SpeakerBio: Wan Ding Yao, AI Security Lead at Singapore GovTech's Cyber Security Group

Mr Wan Ding Yao is the AI Security Lead in Singapore GovTech's Cyber Security Group driving workstreams at the intersection of AI and cybersecurity including prototyping AI use cases for cybersecurity operations and developing AI red-teaming capabilities. He holds a Bachelor of Laws (Technology for Business) and a Master of Science in Computing (Data Science & Engineering) from the Singapore Management University. He is admitted to the Singapore Bar and holds professional cybersecurity certifications from OffSec, CREST, (ISC)2, Practical DevSecOps, MAD20, AWS, Microsoft, and Google.

SpeakerBio: Christine Lai, Cybersecurity Research Specialist at DHS Cyber Security and Infrastructure Security Agency

Christine Lai is a cybersecurity research specialist in the Office of the Technical Director at the Cybersecurity and Infrastructure Security Agency (CISA), where she currently serves as the AI Security lead for the agency. Prior to joining CISA, she was a cybersecurity and machine learning researcher on critical infrastructure programs at Sandia National Laboratories in Albuquerque, NM.

SpeakerBio: Anjuli Shere, Head of Cyber Advocacy in the Cyber Security at Directorate of the UK's Department for Science, Innovation and Technology

Dr. Anjuli Shere is the Head of Cyber Advocacy in the Cyber Security Directorate of the UK's Department for Science, Innovation and Technology. She has a doctorate in Cyber Security from the University of Oxford, during which she spent two years as a Research Fellow at Harvard Kennedy School's Shorenstein Center on Media, Politics and Public Policy. Dr.Shere's research covered emerging technological risks, focusing on converging threats to journalists and media freedom from the consumer Internet of Things in Taiwan, Australia, the U.K. and the U.S. Additionally, she was an intelligence analyst on Channel 4's fugitive simulations "Hunted" and "Celebrity Hunted" for seven series (2017-2025), and an expert advisor to the Financial Times Film "People You May Know" about surveillance during the COVID-19 pandemic. Dr. Shere's previous relevant experience also includes tech/politics writing for the New Statesman, working as a research analyst at the Association for International Broadcasting, and honing her skills in analysis and investigation as part of CyberPATH (the UK National Cyber Resilience Centres Programme) and as a "Digital Sherlock" with the Atlantic Council's Digital Forensic Research Lab.

Return to Index - Add to Google - ics Calendar file

Title: How Competitions Can Fuel Innovation
When: Friday, Aug 9, 17:20 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Fireside Chat with Past Challenge Participants

Speakers: Mike Walker,Matt Knight,Ruoyu "Fish" Wang

SpeakerBio: Mike Walker, Senior Director at Microsoft Research
Mike Walker is a Senior Director at Microsoft Research building special projects:

- Project Freta – A prototype exploration of automated memory introspection: trusted sensing of threats to power the future of automated cloud defense.
- Fuzzing for Developers – An open source self-hosted developer fuzzing platform for Azure developed in partnership with many of Microsoft's core product teams.

Prior to joining Microsoft, Mike led DARPA's Cyber Grand Challenge, a two-year $58M contest to construct & compete the first prototypes of reasoning cyberdefense AI. In 2016 at the DEF CON hacking contest, these prototypes took their first flight into the game of hackers, Capture the Flag, landing zero-day exploits and writing patches in a fully autonomous battle. Read about these AI prototypes in the New York Times (opens in new tab), Wired, and Popular Science (opens in new tab) or watch Mike on 60 Minutes (opens in new tab).

Mike has worked in a policy advisory role, testifying to the President's Commission on Cybersecurity and serving as contributor and panelist to CNAS's Surviving on a Diet of Poisoned Fruit. Prior to joining DARPA he worked as a research lab leader and principal vulnerability researcher focusing on tools to bring the power of supercompute automation to the field of software safety.

As a principal at the Intrepidus Group, Mike worked on Red Teams that tested America's financial and energy infrastructure for security weaknesses. As part of the DARPA SAFER Red Team, Mike discovered flaws in prototype anonymity technologies.

Mike has played in and designed globally competitive hacking contests ("CTF") and coached competitive hacking teams throughout his career.

SpeakerBio: Matt Knight, Head of Security at OpenAI
No BIO available
SpeakerBio: Ruoyu "Fish" Wang, Assistant Professor at School of Computing and Augmented Intelligence
No BIO available

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 11:25-12:15 PDT

Title: How do we make LLVM quantum?
When: Friday, Aug 9, 11:25 - 12:15 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

There are many hurdles we have to solve before we can make Quantum Computing a part of our everyday lives. Yes, we need to work out how to build it, and what we're actually going to run on it, but ignore that for now: we also need to figure out how we program it.

Up until now most quantum programming frameworks have been written in Python, and simply serialize to simplistic string-based representations that are sent over a REST API to cloud-connected quantum hardware. But this ignores the history of classical programming infrastructure, and the fact that no algorithm is purely quantum -- there is bound to be expensive and interwoven classical processing, and we need to take this into account.

Josh will chat about how we are planning to bring quantum to the existing LLVM compiler toolchain, show what quantum programming and compilation looks like today (and in the future!), and how you might be able to help us build it.

SpeakerBio: Josh Isaac

Josh Izaac is a theoretical physicist and Director of Product at Xanadu, and previously led Xanadu's quantum software development, including Strawberry Fields, a platform for photonic quantum computing, and PennyLane, an open-source quantum machine learning software library. At Xanadu, he contributes to the development and growth of Xanadu's open-source quantum software products. Josh holds a PhD in quantum computing and computational physics from the University of Western Australia.

Return to Index - Add to Google - ics Calendar file

CHV - Friday - 14:30-14:59 PDT

Title: How I discovered and hacked Learning Codes of the key job of a car assembled in my country
When: Friday, Aug 9, 14:30 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Using hardware hacking techniques, it was possible to detect the use of learning codes instead of rolling codes in a key job of a car widely used in my country. For this purpose, the key job was disassembled and the HS2240 integrated circuit was detected and, using a logic analyzer, the emission of learning codes from the integrated circuit to the radio frequency LED emitter was checked. With the use of HackRF SDR, the learning code is duplicated to be able to open the car N times without needing the original key anymore, which proves that the use of learning codes is very vulnerable, just like fixed codes.

SpeakerBio: Danilo Erazo, Ethical Hacker at Fluid Attacks

Electronics and Computer Networks Engineer. He works as an Ethical Hacker at Fluid Attacks where he performs Web Pentesting, Cloud Pentesting, Mobile Pentesting, among others. In his free time he dedicates himself to research in the area of hardware/radio frequency/car hacking. He has had the opportunity to be a speaker at international cybersecurity events such as Ekoparty 2023 Argentina, Flisol Ecuador, Hack4all Chile, Bsides Colombia 2024, Nerdearla Chile 2024, among others.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 15:05-16:05 PDT

Title: How I Learned to Stop Worrying and Love the Ban
When: Saturday, Aug 10, 15:05 - 16:05 PDT
Where: Virtual

Description:
SpeakerBio: Manfred

Manfred started out by taking apart toasters and breaking things to find out how they worked. That curiosity moved to client-server authoritative online games and snowballed into a 20+ year career operating in the dark alleys of shadow markets. Manfred has been in the trenches of hacking online games while building out a toolbelt to keep an upper hand in the ever changing cheat vs anti cheat arms race.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 16:30-17:59 PDT

Title: How is GenIA Impacting Cybersecurity: The good, The Bad, and The ugly (Trilingual Panel)
When: Saturday, Aug 10, 16:30 - 17:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Con la presentacion de diferentes expertos en el tema, los cuales en este panel presentado en tres idiomas, vamos a discutir el impacto real que genera la GenIA en nuestro mundo de cibserseguridad

SpeakerBio: Marco Figueroa
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-10:59 PDT

Title: How to Corrupt Youth to Cyber Focused Space Science
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

Bringing cyber focused space science to schools can be challenging given school restrictions, firewalls, and expense of equipment. This presentation will go over multiple space-centric outreach activities for youth of all ages. From talking to astronauts aboard the International Space Station (ISS) to listening to satellites in the classroom. These various programs are bound to capture the imagination. Some of the projects to be discussed are the Amateur Radio on the International Space Station (ARISS) program, Slow-Scan Television (SSTV) images from the ISS, AMSat CubeSat Simulators, and setting up a RTL-SDR to capture information from satellites in the classroom. There are a variety of ways to start a countdown to space science careers in youth and these projects can help you connect with the imagination of youth near you.

SpeakerBio: RC Jones

RC, a cybersecurity researcher focusing on the cybersecurity of space systems. She is currently a PhD student in Aerospace Sciences and holds an Amateur Radio Extra class License. Additionally she supports the Amateur Radio on the International Space Station (ARISS) Education committee and frequently facilitates “Teach the Teacher” workshops for K-12 educators and Youth Outreach leads.

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 14:00-14:59 PDT

Title: How to Find a 0day in iOS Apps
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

This talk delves into the methodologies and strategies for discovering zero-day vulnerabilities in iOS applications. It covers the fundamental principles of iOS security, including code review, reverse engineering, and dynamic analysis techniques. Attendees will gain insights into common weaknesses in iOS app architecture and learn how to exploit these vulnerabilities ethically. By the end of the session, participants will be equipped with practical tools and knowledge to identify and address potential security threats in iOS applications.

SpeakerBio: Xavier D. Johnson, Security Researcher

Born and raised in Detroit, a self-starter from the heart of the Motor City. I took the initiative to teach myself programming in 2004, setting the stage for a trajectory that would shape my future. During my high school years, I proudly served as the President of my school's engineering academy, where my leadership skills and innovative mindset grew. Post-graduation, I ventured into the business world, founding a successful software company that I later sold. My transition into the realm of cybersecurity was a natural evolution, and I have since dedicated myself to security research. I founded Build Skill Foundation, a non-profit organization committed to empowering individuals through education and mentorship. My personal methodology, honed over years of self-directed learning, serves as the backbone of this foundation. In the spirit of Detroit's resilience, I am not just forging my own path but paving the way for others to follow, making a lasting impact on the world of technology and education.

Return to Index - Add to Google - ics Calendar file

Title: How to Steal Voting Software and Get Away With It
When: Friday, Aug 9, 11:45 - 12:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

In 2021, Georgia's voting system suffered the most severe security breach known in US history when partisan operatives entered the election offices in Coffee County, a small county in south Georgia, and took forensic images of all components of the voting system. And because Georgia uses one voting system statewide, the software stolen from Coffee is the same in use across the state. Remarkably, even though the crimes were caught on surveillance camera, the security breach did not come to light until 15 months later, when the plaintiffs in the civil litigation, Curling v. Raffensperger uncovered not just the surveillance camera footage, but emails, documents and contracts that showed this was an extensive and coordinated plot to unlawfully take voting software from Georgia and other states too. Despite the extensive evidentiary record the plaintiffs have developed, neither the local DA or the state Attorney General sought to charge these crimes. However, Fulton County District Attorney Fani Willis included computer trespass, computer identity theft and computer theft alleged in Coffee County as predicate crimes in her RICO indictment, charging four individuals specifically with that element of the conspiracy. Two of those charged, Sidney Powell and Scott Hall, have pleaded guilty. This panel will explain how these events took place, and how they were uncovered, not by the Secretary of State, other election officials or federal or Georgia law enforcement; but by a small non-profit and its fellow plaintiffs and attorneys in civil litigation. The presentation will also discuss how these events are connected to other voting system software breaches in other states, and what this could mean for the 2024 elections and beyond.

Speakers: Susan Greenhalgh,Anna Bower,Rich DeMillo,Marilyn Marks

SpeakerBio: Susan Greenhalgh

Susan Greenhalgh is the Senior Advisor on Election Security for Free Speech For People. Ms. Greenhalgh has previously served as vice president of programs at Verified Voting and at the National Election Defense Coalition, advocating for secure election protocols, paper ballot voting systems and post-election audits. Recognized as an expert on election security, she has been invited to testify before the U.S. Commission on Civil Rights and has been an invited speaker at meetings of the MITRE Corporation, the National Conference of State Legislatures, the Mid-West Election Officials Conference, the International Association of Government Officials, the Election Verification Network and the E-Vote-ID conference in Bregenz, Austria. She is a frequent source for reporters from The New York Times, The Washington Post, The

Wall Street Journal, Politico, USA Today, Associated Press, National Public Radio and other leading news outlets. She has appeared on CNN and MSNBC's The Rachel Maddow Show, and various other television news shows. She has a BA in Chemistry from the University of Vermont.

SpeakerBio: Anna Bower

Anna Bower is Lawfare's Legal Fellow and Courts Correspondent. Anna holds a Bachelor of Laws from the University of Cambridge and a Juris Doctorate from Harvard Law School. She joined Lawfare as a recipient of Harvard's Sumner M. Redstone Fellowship in Public Service. Prior to law school, Anna worked as a judicial assistant for a Superior Court judge in the Northeastern Judicial Circuit of Georgia. She also previously worked as a Fulbright Fellow at Anadolu University in Eskişehir, Turkey. A native of Georgia, Anna is based in Atlanta and Washington, D.C.

SpeakerBio: Rich DeMillo

Richard DeMillo is the Charlotte B. and Roger C. Warren Chair in Computing at the Georgia Institute of Technology. With Cybersecurity threats on the rise, he founded and led Georgia Tech's School of Cybersecurity and Privacy, the first-of-a-kind

at a top research university. He was formerly the John P. Imlay Dean of Computing. Positions he held before joining Georgia Tech include Chief Technology Officer for Hewlett-Packard, Vice President of Computing Research for Bell Communications Research, Director of the Computer Research Division for the National Science Foundation, and Director of the Software Test and Evaluation Project for the Office of the Secretary of Defense. He has also held faculty positions at the University of Wisconsin, Purdue University, and the University of Padua, Italy.

SpeakerBio: Marilyn Marks

Is a retired CEO of a truck-trailer manufacturing business, applying business and leadership skills to election policy reform. In 2009, after a narrow loss to become the Mayor of Aspen, Marilyn recognized the vulnerabilities in Colorado's election systems. She then devoted full time to election integrity litigation and lobbying efforts for more transparent and verifiable elections. She successfully litigated the effort to make Colorado ballots open public records for post-election reviews, followed by dozens of election-related cases involving election security, transparency, and voter privacy. After moving back east to North Carolina, her focus became primarily CGG's work in southern states, including Georgia, where CGG has intensely focused on Georgia's insecure and unauditable electronic voting system and the anti-democratic and anti-transparency provisions of SB202 passed in 2021.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 13:30-14:15 PDT

Title: How we built our REDACTED THING this year, 5n4ck3y, && AMA Panel on Making Badges
When: Saturday, Aug 10, 13:30 - 14:15 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

See talk title, kids these days dont read more than a sentence anyway. Seriously though, we get asked a lot of random custom electronics, hardware hacking, and badge questions, here's your chance to throw them at us while we drink a beer and pretend to know the right answer

SpeakerBio: AND!XOR

AND!XOR is a hacker group of engineers who make electronic badges, retrofit snack machines, shenanigans, and other useful tech such as the wireless microwave oven sensor.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: HTB CTF: Data Dystopia
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06 - Map

Description:

A powerful corporation, notorious for its unethical practices, leveraged their extensive data resources gathered from users, and their psychological profiles, to subdue the population into compliance. The immune few, realizing the extent of the corporate conspiracy, band together to expose and dismantle the corporation's grip on society. These individuals must navigate a dangerous world of surveillance and betrayal. Their mission is to ignite a global awakening and reclaim freedom from corporate domination.

Players will have to join the mission and participate in a CTF that would be beneficial for beginners and experienced players alike. The challenge categories will be Web, Cryptography, Forensics, PWN(binary exploitation) and Reverse Engineering. Various difficulty challenges from each category will be featured.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: HTB CTF: Data Dystopia
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06 - Map

Description:

A powerful corporation, notorious for its unethical practices, leveraged their extensive data resources gathered from users, and their psychological profiles, to subdue the population into compliance. The immune few, realizing the extent of the corporate conspiracy, band together to expose and dismantle the corporation's grip on society. These individuals must navigate a dangerous world of surveillance and betrayal. Their mission is to ignite a global awakening and reclaim freedom from corporate domination.

Players will have to join the mission and participate in a CTF that would be beneficial for beginners and experienced players alike. The challenge categories will be Web, Cryptography, Forensics, PWN(binary exploitation) and Reverse Engineering. Various difficulty challenges from each category will be featured.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: HTB CTF: Data Dystopia
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06 - Map

Description:

A powerful corporation, notorious for its unethical practices, leveraged their extensive data resources gathered from users, and their psychological profiles, to subdue the population into compliance. The immune few, realizing the extent of the corporate conspiracy, band together to expose and dismantle the corporation's grip on society. These individuals must navigate a dangerous world of surveillance and betrayal. Their mission is to ignite a global awakening and reclaim freedom from corporate domination.

Players will have to join the mission and participate in a CTF that would be beneficial for beginners and experienced players alike. The challenge categories will be Web, Cryptography, Forensics, PWN(binary exploitation) and Reverse Engineering. Various difficulty challenges from each category will be featured.

Return to Index - Add to Google - ics Calendar file

PLV - Friday - 14:30-15:15 PDT

Title: Human Dignity in AI and Tech Policy
When: Friday, Aug 9, 14:30 - 15:15 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Social media have been a decade-long dress rehearsal in online manipulation. AI can create information, make predictions and take decisions that will affect human behaviour, including our behaviours as citizens, workers and consumers. Safeguards are needed, since generative AI will only exacerbate the personal, social and societal harms already caused by data-driven business models.

We examine the centrality of human dignity in tech law and policy and how our mindsets and legal frameworks must be informed by psychological, technological and societal perspectives. Based on insights from market dynamics, marketing techniques, design strategies, and human frailties we demonstrate how information asymmetries have reduced individual agency and the ability to create transparency.

Human dignity is a core value in liberal democracies that must also be reflected in tech policy. Protections are required when businesses interfere with our rights to freedom, property, privacy and non-discrimination. With the digitalisation of the human experience, users have become programmable objects. We cannot rely on regulation alone and need to discuss how we can act to reclaim our dignity.

SpeakerBio: Jan Trzaskowski, Law Professor at Aalborg University and Copenhagen Business School

Jan Trzaskowski, PhD, is Law Professor at Aalborg University and Copenhagen Business School and author of the important and successful book Your Privacy Is Important to Us! – Restoring Human Dignity in Data-Driven Marketing [as well as many other books, chapters and articles]. Since the mid-1990s, he has dealt with legal and regulatory aspects of information technology, and his research focuses on the protection of consumers and fundamental rights, including privacy. He has a keen interest in human decision-making (psychology and marketing) and the role of persuasive technology. Currently, he focuses on the regulation of AI and data-driven business models, including the role of human dignity and fundamental rights impact assessments. He was Head of the Danish delegation negotiating the 2000 E-Commerce Directive, and as a kid he wrote Commodore 64 assembly language routines that were published in Danish computer magazine IC RUN.

Return to Index - Add to Google - ics Calendar file

Title: Human Registration Open
When: Sunday, Aug 11, 08:00 - 15:59 PDT
Where: LVCC West - Map

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- $480 online purchase until August 1, 2024. Tickets are transferable. Please read the details on the linked page.
- $460 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are

picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: $34 until July 15, and $84 on and after July 15.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you attend BlackHat, it is possible to purchase a DEF CON badge with your BlackHat registration. If you did so, please get your DEF CON badge from BlackHat before they close.

BlackHat should send you an email with instructions for how to obtain your DEF CON badge. In case you missed it, you can go to the second floor, at the concierge desk, halfway down Black Hat Blvd.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

Title: Human Registration Open
When: Thursday, Aug 8, 08:00 - 19:59 PDT
Where: LVCC West - Map

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- $480 online purchase until August 1, 2024. Tickets are transferable. Please read the details on the linked page.
- $460 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are

picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: $34 until July 15, and $84 on and after July 15.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you attend BlackHat, it is possible to purchase a DEF CON badge with your BlackHat registration. If you did so, please get your DEF CON badge from BlackHat before they close.

BlackHat should send you an email with instructions for how to obtain your DEF CON badge. In case you missed it, you can go to the second floor, at the concierge desk, halfway down Black Hat Blvd.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

Title: Human Registration Open
When: Friday, Aug 9, 08:00 - 19:59 PDT
Where: LVCC West - Map

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- $480 online purchase until August 1, 2024. Tickets are transferable. Please read the details on the linked page.
- $460 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are

picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: $34 until July 15, and $84 on and after July 15.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you attend BlackHat, it is possible to purchase a DEF CON badge with your BlackHat registration. If you did so, please get your DEF CON badge from BlackHat before they close.

BlackHat should send you an email with instructions for how to obtain your DEF CON badge. In case you missed it, you can go to the second floor, at the concierge desk, halfway down Black Hat Blvd.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

MISC - Saturday - 08:00-18:59 PDT

Title: Human Registration Open
When: Saturday, Aug 10, 08:00 - 18:59 PDT
Where: LVCC West - Map

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- $480 online purchase until August 1, 2024. Tickets are transferable. Please read the details on the linked page.
- $460 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are

picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: $34 until July 15, and $84 on and after July 15.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you attend BlackHat, it is possible to purchase a DEF CON badge with your BlackHat registration. If you did so, please get your DEF CON badge from BlackHat before they close.

BlackHat should send you an email with instructions for how to obtain your DEF CON badge. In case you missed it, you can go to the second floor, at the concierge desk, halfway down Black Hat Blvd.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

BBV - Saturday - 11:30-12:30 PDT

Title: Hunters and Gatherers: A Deep Dive into the World of Bug Bounties
When: Saturday, Aug 10, 11:30 - 12:30 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Join us for an insightful panel discussion where we bring together seasoned Bug Bounty Program Managers and adept bug bounty hunters. This panel aims to address pressing questions and share diverse perspectives on the evolving landscape of bug bounties. We will dive into the challenges faced by both hunters and managers, discuss strategies to enhance the impact of submissions, and explore the future of bug bounties in the face of emerging technologies, evolving trends, and threats. We will also highlight the importance of bug bounties in the current cybersecurity landscape and share the top elements that contribute to a successful bug bounty program. Lastly, we will provide recommendations for organizations looking to mature their bug bounty programs but are hesitant about expanding. This panel promises to be a valuable opportunity for learning, sharing, and networking for anyone involved or interested in the world of bug bounties.

Speakers: Johnathan Kuskos,Katie Trimble-Noble,Sam (erbbysam) Erb,Jeff Guerra,Logan MacLaren

SpeakerBio: Johnathan Kuskos, Founder at Chaotic Good Information Security (CGIS)

There's no place Kuskos would rather be than somewhere with a cool breeze, lightning-fast bandwidth, a decent brew, and a list of servers to target . He discovered his passion for offensive security nearly 13 years ago and quickly became obsessed with the art of finding overlooked vulnerabilities, understanding why they're missed, and enhancing tools and methodologies for comprehensive coverage. Kuskos is the founder of Chaotic Good Information Security, a labor of love boutique penetration testing firm.

SpeakerBio: Katie Trimble-Noble, Director PSIRT & Bounty

Director, PSIRT and Bug Bounty at a Fortune 50 tech Company. Katie serves as a CVE Program Board, Bug Bounty Community of Interest Board, and Hacking Policy Council member. She is a passionate defensive cybersecurity community activist, she is regularly involved is community driven projects and is most happy when she is able to effect positive progress in cyber defense. Prior to joining private sector, Katie spent over 15 years in the US Government. Most recently as the Section Chief of Vulnerability Management and Coordination at the Department of Homeland Security, Cyber and Infrastructure Security Agency (CISA).

SpeakerBio: Sam (erbbysam) Erb, Security Engineer at Google

Sam is a security engineer at Google who helps run the Google and Alphabet Vulnerability Reward Program. He holds two DEFCON black badges and numerous bug bounty live hacking event awards. He has presented previously on the DEFCON main stage and in the Packet Hacking Village. Outside of hacking, you will likely find Sam in a climbing gym or on the side of a mountain.

SpeakerBio: Jeff Guerra, Sr. Product Security Engineer at GitHub

Jeff Guerra is a Sr. Product Security Engineer at GitHub who enjoys bounties, application security, and much more. He is an avid advocate for vulnerability disclosure/bug bounty programs and the effectiveness and community engagement that comes with it. He's a curious and passionate security professional who loves to talk all things security. He loves watching and playing soccer and has recently began his journey into time-attack track events. He's a huge car enthusiast and recently began learning to modify cars for the track and daily use.

SpeakerBio: Logan MacLaren, Senior Product Security Engineer at GitHub

Logan is a Senior Product Security Engineer at GitHub where he focuses on the success of their Bug Bounty program. When not hacking on GitHub itself, Logan can be found doing security research focused on open source projects, or learning and refining new skills with CTF challenges!

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 12:00-12:30 PDT

Title: I am still the Captain now!
When: Saturday, Aug 10, 12:00 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Fresh from his DEFCON 31 marsec village talk, 'I am the Captain now', Paul has another year's experience at sea from which to share stories of taking control of vessels.

As it's timely, he will look at why the MV Dali incident wasn't a hack, dispelling ill-informed opinions from the wave of armchair experts that suddenly emerged, but more interestingly, ways that it so easily could have been a cyber event.

Finally, maritime cyber regulation is starting to catch up, but so many operators and technology providers are likely to be caught out by IACS UR E26 & 27

SpeakerBio: Paul Brownridge
No BIO available

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 15:15-15:59 PDT

Title: I've got 99 problems but a prompt injection ain't pineapple
When: Saturday, Aug 10, 15:15 - 15:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

The ethical and secure disclosure of vulnerabilities in AI has emerged as a pivotal challenge, compounded by the need to address biases and misinformation that often cloud the true nature of these vulnerabilities. This talk delves into the intricate dynamics of vulnerability disclosure within AI, balancing transparency with security. We'll dissect the unique challenges AI presents, such as data bias exploitation and model manipulation, which can amplify the impact of vulnerabilities. Through a lens of real-world examples and recent disclosures, we'll navigate the complexities of responsible vulnerability management in AI. Our discussion will not only aim to shed light on these critical issues but also inspire a unified approach to refining disclosure processes. This concerted effort is vital for enhancing the integrity of AI systems and bolstering public trust in their use.

Speakers: Chloé Messdaghi,Kasimir Schulz

SpeakerBio: Chloé Messdaghi, Head of Threat Intelligence at HiddenLayer

Chloé Messdaghi is the Head of Threat Intelligence at HiddenLayer, leading efforts to secure AI measures and promote industry-wide security practices. A sought-after public speaker and trusted authority for journalists, her expertise has been widely featured in the media. Recognized as a Power Player by Business Insider and SC Media, Chloé has made significant contributions to cybersecurity. Outside of work, she is dedicated to philanthropy, advancing industry progress, and promoting societal and environmental well-being.

Chloé Messdaghi serves as the Head of Threat Intelligence at HiddenLayer, where she spearheads efforts to fortify security for AI measures and fosters collaborative initiatives to enhance industry-wide security practices for AI. A highly sought-after public speaker and trusted authority for national and sector-specific journalists, Chloé's expertise has been prominently featured across various media platforms. Her impactful contributions to cybersecurity have earned her recognition as a Power Player by esteemed publications such as Business Insider and SC Media.Beyond her professional endeavors, Chloé remains passionately committed to philanthropy aimed at advancing industry progress and fostering societal and environmental well-being.

SpeakerBio: Kasimir Schulz, Principal Security Researcher at HiddenLayer

Kasimir Schulz, Principal Security Researcher at HiddenLayer, is a leading expert in uncovering zero-day exploits and supply chain vulnerabilities in AI. His work has been featured in BleepingComputer and Dark Reading, and he has spoken at conferences such as FS-ISAC and Black Hat. Kasimir leads the development of advanced tools for automating vulnerability detection and implementing large-scale patches, fortifying systems against supply chain attacks. His dedication to proactive defense measures sets a new standard in cybersecurity resilience.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 16:15-16:45 PDT

Title: I've got 99 problems but a prompt injection ain't watermelon
When: Friday, Aug 9, 16:15 - 16:45 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

The ethical and secure disclosure of vulnerabilities in AI has emerged as a pivotal challenge, compounded by the need to address biases and misinformation that often cloud the true nature of these vulnerabilities. This talk delves into the intricate dynamics of vulnerability disclosure within AI, balancing transparency with security. We'll dissect the unique challenges AI presents, such as data bias exploitation and model manipulation, which can amplify the impact of vulnerabilities. Through a lens of real-world examples and recent disclosures, we'll navigate the complexities of responsible vulnerability management in AI. Our discussion will not only aim to shed light on these critical issues but also inspire a unified approach to refining disclosure processes. This concerted effort is vital for enhancing the integrity of AI systems and bolstering public trust in their use.

Speakers: Chloé Messdaghi,Kasimir Schulz

SpeakerBio: Chloé Messdaghi, Head of Threat Intelligence at HiddenLayer

Chloé Messdaghi is the Head of Threat Intelligence at HiddenLayer, leading efforts to secure AI measures and promote industry-wide security practices. A sought-after public speaker and trusted authority for journalists, her expertise has been widely featured in the media. Recognized as a Power Player by Business Insider and SC Media, Chloé has made significant contributions to cybersecurity. Outside of work, she is dedicated to philanthropy, advancing industry progress, and promoting societal and environmental well-being.

Chloé Messdaghi serves as the Head of Threat Intelligence at HiddenLayer, where she spearheads efforts to fortify security for AI measures and fosters collaborative initiatives to enhance industry-wide security practices for AI. A highly sought-after public speaker and trusted authority for national and sector-specific journalists, Chloé's expertise has been prominently featured across various media platforms. Her impactful contributions to cybersecurity have earned her recognition as a Power Player by esteemed publications such as Business Insider and SC Media.Beyond her professional endeavors, Chloé remains passionately committed to philanthropy aimed at advancing industry progress and fostering societal and environmental well-being.

SpeakerBio: Kasimir Schulz, Principal Security Researcher at HiddenLayer

Kasimir Schulz, Principal Security Researcher at HiddenLayer, is a leading expert in uncovering zero-day exploits and supply chain vulnerabilities in AI. His work has been featured in BleepingComputer and Dark Reading, and he has spoken at conferences such as FS-ISAC and Black Hat. Kasimir leads the development of advanced tools for automating vulnerability detection and implementing large-scale patches, fortifying systems against supply chain attacks. His dedication to proactive defense measures sets a new standard in cybersecurity resilience.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 13:30-14:25 PDT

Title: iCLASS - Throwing away the keys
When: Friday, Aug 9, 13:30 - 14:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

RFID PACS systems are used to secure doors to airports, server rooms, and other high security facilities, but the security is often more marketing than reality. This talk will reveal a new media authentication bypass vulnerability in HID iCLASS and Signo physical access control system RFID readers that has existed for over a decade and the journey of initial discovery, disbelief, vendor disclosure, and patch. While legacy iCLASS has been known to be compromised for years thanks to the research presented in Milosch Meriac's "Heart of Darkness" and Flavio D. Garcia's "Dismantling iCLASS and iCLASS Elite" for standard and elite keys respectively. iCLASS SE systems have had a presumed level of security over legacy iCLASS at least as far as direct attacks that don't involve additional techniques such as downgrading.

SpeakerBio: Tiernan "nvx" Messmer

Tiernan grew up watching DEF CON talks online and has always enjoyed breaking and bypassing security for fun. By day he works as a software engineer for a not-for-profit, by night he enjoys tinkering, contributing to open-source software, and reverse engineering things that companies would sometimes rather he didn't. He prefers to hack on software but doesn't mind getting his hands dirty with hardware when needed. Tiernan believes the best way to determine if he really understands something is if he can successfully explain it to either someone else or create a working implementation in code. This has led him to develop iCLASS/PicoPass card emulation on the Chameleon Tiny/Mini and the Flipper Zero. In recent years he has become a "Hero" of the "RFID Hacking by Iceman" Discord going by "NVX" and can be found on GitHub as nvx.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 17:30-18:15 PDT

Title: Iconv, set the charset to RCE: exploiting the glibc to hack the PHP engine
When: Saturday, Aug 10, 17:30 - 18:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Upon its discovery, CVE-2024-2961, a very old buffer overflow in the glibc, seemed like a terrible bug. Within the prism of the PHP engine, however, the vulnerability shone, and provided both a new remote code execution vector and a few 0-days.

This talk will first walk you through the discovery of the bug and its limitations, before describing the conception of remote binary PHP exploits using this bug, and through them offer unique insight in the internal of the engine of the web language, and the difficulties one faces when exploiting it.

After this, it will reveal the impact on PHP's ecosystem, from well-known functions to unsuspected sinks, by showcasing the vulnerability on several popular libraries and applications.

SpeakerBio: Charles "cfreal" Fol, Security Researcher at LEXFO / AMBIONICS

Charles Fol, also known as cfreal, is a security researcher at LEXFO / AMBIONICS. He has discovered remote code execution vulnerabilities targeting renowned CMS and frameworks such as Drupal, Magento, Symfony or Laravel, but also enjoys binary exploitation, to escalate privileges (Apache, PHP-FPM) or compromise security solutions (DataDog's Sqreen, Fortinet SSL VPN, Watchguard). He is the creator for PHPGGC, the go-to tool to exploit PHP deserialization, and an expert in PHP internals.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 16:30-16:59 PDT

Title: ICS 101
When: Friday, Aug 9, 16:30 - 16:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Introduction to industrial control systems:
- What is ICS
- Purdue model
- How ICS is architected
- Attacker view of ICS architecture
- How to build your own ICS lab
- Equipment
- How to learn / conduct vulnerability research

Speakers: Bryson Bort ,Tom VanNorman

SpeakerBio: Bryson Bort
No BIO available

SpeakerBio: Tom VanNorman, ICS Village
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: ICS CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The ICS Village CTF offers hands-on experiences with industrial control systems, which bridge technology with physics. Attendees engage with industry experts while solving challenges like a red vs blue manufacturing network process coupled with OT-specific jeopardy-stye challenges. This contest highlights vulnerabilities in industrial equipment and OT protocols. By simulating attacks on critical infrastructure, participants develop and practice DEFCON-level skills, enhancing their understanding with critical infrastructure and the world we rely on.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: ICS CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The ICS Village CTF offers hands-on experiences with industrial control systems, which bridge technology with physics. Attendees engage with industry experts while solving challenges like a red vs blue manufacturing network process coupled with OT-specific jeopardy-stye challenges. This contest highlights vulnerabilities in industrial equipment and OT protocols. By simulating attacks on critical infrastructure, participants develop and practice DEFCON-level skills, enhancing their understanding with critical infrastructure and the world we rely on.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: ICS CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The ICS Village CTF offers hands-on experiences with industrial control systems, which bridge technology with physics. Attendees engage with industry experts while solving challenges like a red vs blue manufacturing network process coupled with OT-specific jeopardy-stye challenges. This contest highlights vulnerabilities in industrial equipment and OT protocols. By simulating attacks on critical infrastructure, participants develop and practice DEFCON-level skills, enhancing their understanding with critical infrastructure and the world we rely on.

Return to Index - Add to Google - ics Calendar file

XRV - Friday - 10:00-17:59 PDT

Title: ICS Village + XR Village Turn the lights on!
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

Idaho National Laboratory in collaboration with the Cybersecurity & Infrastructure Security Agency (CISA) will showcase the critical importance of safeguarding Industrial Control Systems (ICS) against cyber threats. Through a mixed reality game, the interactive VR experience illustrates the impacts of a cybersecurity attack on infrastructure, and highlights the intricate engineering processes that power our communities. By emphasizing the interdependencies within our Nation's infrastructure, the VR challenges underscore the necessity of robust cybersecurity measures to ensure the reliability and security of essential services. Come restore power back to our city, virtually! (NOTE: this gamified interactive VR experience not technical in nature, and does not require cybersecurity or infrastructure knowledge to participate

Return to Index - Add to Google - ics Calendar file

XRV - Saturday - 10:00-17:59 PDT

Title: ICS Village + XR Village Turn the lights on!
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

Idaho National Laboratory in collaboration with the Cybersecurity & Infrastructure Security Agency (CISA) will showcase the critical importance of safeguarding Industrial Control Systems (ICS) against cyber threats. Through a mixed reality game, the interactive VR experience illustrates the impacts of a cybersecurity attack on infrastructure, and highlights the intricate engineering processes that power our communities. By emphasizing the interdependencies within our Nation's infrastructure, the VR challenges underscore the necessity of robust cybersecurity measures to ensure the reliability and security of essential services. Come restore power back to our city, virtually! (NOTE: this gamified interactive VR experience not technical in nature, and does not require cybersecurity or infrastructure knowledge to participate

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 11:10-11:50 PDT

Title: Identity Theft is not a Joke, Azure!
When: Saturday, Aug 10, 11:10 - 11:50 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

As Azure services continue to expand and evolve, their associated authentication methodologies have also changed. Having mostly moved away from storing credentials in cleartext, most Azure services utilize Managed Identities to offer a more secure approach to access management. However, Managed Identities can bring their own challenges and risks. In this talk, we delve into the nuanced landscape of Managed Identities across multiple Azure services. We explore how attackers exploit access to services with these identities to escalate privileges, move laterally, and establish persistence within Azure tenants. We will also provide helpful tips for defenders trying to identify these attacks. Finally, we will showcase a tool designed to automate attacks against User-Assigned Managed Identities.

SpeakerBio: Karl Fosaaen

As a VP of Research, Karl is part of a team developing new services and product offerings at NetSPI. Karl previously oversaw the Cloud Penetration Testing service lines at NetSPI and is one of the founding members of NetSPI's Portland, OR team. Karl has a Bachelors of Computer Science from the University of Minnesota and has been in the security consulting industry for 15 years. Karl spends most of his research time focusing on Azure security and contributing to the NetSPI blog. As part of this research, Karl created the MicroBurst toolkit to house many of the PowerShell tools that he uses for testing Azure. In 2021, Karl co-authored the book "Penetration Testing Azure for Ethical Hackers" with David Okeyode.

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 10:00-10:50 PDT

Title: IDOR in Financial Operations
When: Sunday, Aug 11, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Bank case : Bank A provides an online banking application where users can access their accounts, perform transactions, and initiate money transfers. Here's a scenario with an IDOR vulnerability: Scenario: User A wants to transfer $1000 to User B. User A initiates a transfer and selects the recipient's account. However, due to an IDOR flaw in the application, the validation process fails, allowing users to select other users' accounts. In this case, User A can actually select User B's account and transfer the money, leading to unauthorized access to accounts.

and other cases :)

SpeakerBio: Ilkin Javadov
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: If Existing Cyber Vulnerabilities Magically Disappeared Overnight, What Would Be Next?
When: Friday, Aug 9, 13:00 - 13:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

The DEF CON community challenges the status quo, bringing a diversity of perspectives and ideas to identify hidden problems and solutions. While DARPA lays claim to the origin of the ARPANET/internet, vast communities of people with different interests created its novel components. The DARPA Cyber Grand Challenge helped launch the field of vulnerability detection and remediation and numerous DARPA Cyber Fast Track program performers continue to contribute to DEF CON.

What if current vulnerabilities all magically disappeared overnight and critical infrastructure were “safe and secure” for the time being. What would come next?

In this talk, Dr. Stefanie Tompkins will discuss the value of the hacker community and many of the contributions that have come from it, as well as the growth and synergy of the two communities. She’ll also explore the question of what comes next.

For a deeper dive into the real-world impacts of DARPA cyber technologies, Dr. Renee Wegrzyn, the inaugural director of the Advanced Research Projects Agency for Health (ARPA-H), will join Stefanie and a moderator. They will discuss efforts that impact DEF CON areas of interest and inform ARPA-H work, from Cyber Fast Track to current work focused on securing and defending hospitals and the health tech ecosystem from cyberattacks.

Speakers: Dr. Stefanie Tompkins,Dr. Renee Wegrzyn,Peiter “Mudge” Zatko

SpeakerBio: Dr. Stefanie Tompkins, Director at Defense Advanced Research Projects Agency (DARPA)

Dr. Stefanie Tompkins is the director of the Defense Advanced Research Projects Agency (DARPA). Prior to this assignment, she was the vice president for research and technology transfer at Colorado School of Mines.

Tompkins has spent much of her professional life leading scientists and engineers in developing new technology capabilities. She began her industry career as a senior scientist and later assistant vice-president and line manager at Science Applications International Corporation, where she spent 10 years conducting and managing research projects in planetary mapping, geology, and imaging spectroscopy. As a program manager in DARPA’s Strategic Technology Office, she created and managed programs in ubiquitous GPS-free navigation as well as in optical component manufacturing. Tompkins has also served as the deputy director of DARPA’s Strategic Technology Office, director of DARPA’s Defense Sciences Office – the agency’s most exploratory office in identifying and accelerating breakthrough technologies for national security – as well as the acting DARPA deputy director.

Tompkins received a Bachelor of Arts degree in geology and geophysics from Princeton University and Master of Science and Doctor of Philosophy degrees in geology from Brown University. She has also served as a military intelligence officer in the U.S. Army.

SpeakerBio: Dr. Renee Wegrzyn, First Director at Advanced Research Projects Agency for Health (ARPA-H)

Dr. Renee Wegrzyn is the first director of the Advanced Research Projects Agency for Health (ARPA-H). Bringing a wealth of experience from both the private sector and groundbreaking institutions like DARPA and IARPA, her leadership and vision continue to push the boundaries of health research and development. Dr. Wegrzyn's illustrious career has earned her numerous accolades, including the prestigious Superior Public Service Medal for her contributions at DARPA. She holds a Ph.D. and a bachelor's degree in applied biology from the Georgia Institute of Technology, and she further honed her expertise as an Alexander von Humboldt Fellow in Heidelberg, Germany.

SpeakerBio: Peiter “Mudge” Zatko, Chief Information Officer at DARPA

Peiter “Mudge” Zatko is a distinguished scientist and cybersecurity expert with a career spanning significant roles in both public and private sectors. He returned to DARPA as the agency’s chief information officer in 2024. He previously was a program manager in both the Strategic Technology Office (STO) and Information Innovation Office (I2O). During his tenure in STO, Mudge was pivotal in developing DARPA’s Cyber Analytic Framework, which set a new standard in cybersecurity strategy. He later transitioned to I2O, where he continued to shape DARPA’s cyber initiatives.

Following his impactful career at DARPA, Mudge held key positions in industry, notably serving as corporate vice president of R&D at Motorola Mobility, deputy director at Google’s Advanced Technology and Projects division, and head of security and IT at fintech leader Stripe. Later, Mudge joined the executive team at Twitter, where he oversaw IT, infosec, global platform moderation and services, and corporate security/physical infrastructure.

Most recently, Mudge returned to the public sector as a Senior Government Executive and Senior Executive Service member, reporting to Director Jen Easterly at the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security.

Mudge holds a distinguished record of leadership and innovation in cybersecurity and technology, contributing significantly to both national security and private sector advancements.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 11:00-11:25 PDT

Title: Importance of ICS knowledge from a engineer's perspective
When: Friday, Aug 9, 11:00 - 11:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

In the realm of Operational Technology (OT) environments, incident response is a critical function that ensures the continuity and security of industrial processes. A thorough understanding of vendors, asset types, and associated frameworks is indispensable for effective incident management. This talk underscores the significance of this knowledge from an operator's perspective, highlighting how it can substantially enhance the ability of a cyber security analyst to respond to incidents swiftly and efficiently.

Knowing your vendors and the specific types of assets deployed within an OT environment provides a foundational understanding that is crucial during an incident. Cyber Security analyst's equipped with detailed knowledge of where to locate critical configuration files and logs on OT devices can significantly streamline the incident response process. This insight is vital for establishing baselines, which are essential for detecting anomalies and potential threats. When an incident occurs, the ability to swiftly access and analyze these files can make the difference between a contained event and a widespread disruption.

SpeakerBio: Ray Baeza, Founder at Agriculture Defense Group

Ray Baeza is the founder of Agriculture Defense Group, specializing in cybersecurity services for the agriculture industry. Hailing from Davis, CA, Ray grew up immersed in agriculture. With over 6 years of experience as an ICS cybersecurity engineer, Ray has honed expertise in ICS detection engineering and incident response. Driven by a passion for ICS technologies and the agriculture industry, he is dedicated to safeguarding agricultural systems from cyber threats.

Return to Index - Add to Google - ics Calendar file

MISC - Wednesday - 00:00-00:59 PDT

Title: Important Message
When: Wednesday, Aug 7, 00:00 - 00:59 PDT
Where: Other / See Description

Description:

There are a few things that we would like everyone to be aware of, leading up to DEF CON 32.

Sticker Policy

We have a beautiful culture of #stickerlife at DEF CON, and we hope that it can continue well into the future. Refer to the conference schedule for "sticker swaps". We're also putting up multiple sticker walls this year -- it was a hit last year, and we hope that having a couple of them will be even more awesome this year.

The LVCVA (Las Vegas Convention and Visitors Authority, owners of the LVCC) has a zero-tolerance policy with regard to adhering anything at all to their property, including stickers. Please DFIU. If you are caught adhering anything to LVCC property, you will likely be trespassed from the property by Las Vegas Police. Beyond stickers, you may also not use tape, sticky putty, tacks, or even non-stick clings.

Admission inspections and searches

The LVCC will not be searching or scanning people or bags entering the facility.

Money

As always, human badges (that were not pre-purchased) are exclusively sold using **cash (US currency)**. Merch is the same. No credit cards, debit cards, mobile payments, cryptocurrency, or any means other than USD cash will be accepted at either human registration or DEF CON Merch. We recommend bringing cash with you: there are only two ATMs inside the LVCC.

Food and beverage operations inside the LVCC, including the food court and bars, only accept cards and mobile payments. **You cannot use cash to purchase food or beverage inside the LVCC.**

Vendors are permitted to conduct transactions via whatever means they choose. We do not have a list of which vendors are accepting cash vs card.

Water

The LVCC has many modern water-bottle filling stations, so free water will be readily available for those who bring their own reusable water bottles.

DCTV

DCTV will exclusively be streaming online this year, and will not be available on any hotel TV channels.

Outside food and beverage

LVCC prohibits attendees from bringing outside food and beverage into the convention center, except in cases of medical or dietary necessity.

Photography policy

Public photography is allowed*. It's okay to take photos of your friends if they're cool with it. We've setup several "selfie spots" that are amazing art pieces created specifically for the yearly theme where you can take cool photos.

We want you to take consenting photos of each other and we want others to see the wide range of attendees we have at DEF CON having a good time. What we don't want to see are group shots taken without consent/warning, images taken by the press, video of people standing in lines, etc.

Official Press & DEF CON Policy Village rules may differ, please refer to them. At DEF CON you may see our official photography goons capturing the uniqueness that is to be expected at DEF CON; they adhere to our photo policy.

Groups & individuals participating in public on stage (events, contests, or activities) are allowed* to be photographed.

Photography in the CTF room is NOT permitted without consent of the individuals to be photographed.

Crowd shots are VERY discouraged, if so desired you must alert the crowd to give them time to opt out. For example: " Hey, I'm taking a photo, if you don't want to be in it hide your face" .

Taking photos of people in hallways, lines, hanging out, at random, is not allowed without consent. Respect the rights of the individual not to be photographed. Deletion of photos can be requested by staff.

When taking pictures of your friends please use "portrait mode" because this will blur the picture background, respecting the privacy of those inadvertently captured.

NOTE: It is permissible to record violations of the DEF CON CoC to share with our safety team (link) to help us investigate and take action.

- We reserve the right to revoke an individual's permission to photograph, at any time, on a case by case basis. Failure to comply can result in revocation of admission without refund.

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 10:00-10:30 PDT

Title: Incident Response 101: Part 1 (IR Overview, Lifecycles, Frameworks, and Playbooks)
When: Friday, Aug 9, 10:00 - 10:30 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

This primer on incident response delves into its components, including the necessary procedures, lifecycles, frameworks, and playbooks. Initially, we'll explore the concept of incident response and its requisites. Then, we'll examine the stages of the IR lifecycle and explore adaptable frameworks. Finally, we'll review the strategies and playbooks employed by IR analysts to effectively address incidents.

An introduction to incident response that will focus on a general overview of incident response. Is a security event the same as a security incident? How will I know where to start when a security incident occurs? Although a security incident may unfold swiftly and with intensity, possessing a comprehensive grasp of the Incident Response (IR) process and utilizing frameworks and playbooks can mitigate the pressure inherent in investigating such incidents.

SpeakerBio: Jason Romero

Jason is a skilled cybersecurity professional with over five years of experience in incident response. Throughout this period, he has developed a deep understanding of threat detection, mitigation, and recovery processes. Jason's expertise includes managing security incidents, conducting forensic analysis, and implementing effective response strategies to protect organizations from cyber threats. Known for his analytical skills and ability to work well under pressure, he has successfully led numerous incident response efforts which include adversary groups such as Scattered Spider. Jason is dedicated to stayed ahead of evolving cyber threats and continually enhances his knowledge through ongoing education and hands-on experience.

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 10:30-10:59 PDT

Title: Incident Response 101: Part 2 (Analyst Mindset and Quality Assurance)
When: Friday, Aug 9, 10:30 - 10:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

An introduction to the analyst mindset for IR and how to ensure quality. First, we'll discuss the analyst mindset. How does your investigation flow and potentially impact people? This is a big responsibility. Next we will discuss quality assurance. The "evil" metrics that we so often fear. Why are they important and how can we best use them?

An introduction to the analyst mindset for IR and how to ensure quality. First, we'll discuss the analyst mindset. How does your investigation flow and potentially impact people? This is a big responsibility. Next we will discuss quality assurance. The "evil" metrics that we so often fear. Why are they important and how can we best use them?

SpeakerBio: David "CountZ3r0" Roman

David Roman is a Senior Incident Response Consultant at Cisco Talos Incident Response, with 28 years of experience in the IT and security industry. David leads investigations to help customers on their worst career day recover from security incidents and help them better prepare for the future. Volunteering and helping others learn about cybersecurity is a passion for David. He helps run local DEF CON and CitySec groups and guest lectures at Oklahoma State University.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 13:30-14:15 PDT

Title: Incubated Machine Learning Exploits: Backdooring ML Pipelines Using Input-Handling Bugs
When: Sunday, Aug 11, 13:30 - 14:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Machine learning (ML) pipelines are vulnerable to model backdoors that compromise the integrity of the underlying system. Although many backdoor attacks limit the attack surface to the model, ML models are not standalone objects. Instead, they are artifacts built using a wide range of tools and embedded into pipelines with many interacting components.

In this talk, we introduce incubated ML exploits in which attackers inject model backdoors into ML pipelines using input-handling bugs in ML tools. Using a language-theoretic security (LangSec) framework, we systematically exploited ML model serialization bugs in popular tools to construct backdoors. In the process, we developed malicious artifacts such as polyglot and ambiguous files using ML model files. We also contributed to Fickling, a pickle security tool tailored for ML use cases. Finally, we formulated a set of guidelines for security researchers and ML practitioners. By chaining system security issues and model vulnerabilities, incubated ML exploits emerge as a new class of exploits that highlight the importance of a holistic approach to ML security.

1. link
2. link
3. link
4. link
5. link
6. link
7. link
8. link
9. link
10. link
11. link

SpeakerBio: Suha Sabi Hussain, Security Engineer, Machine Learning Assurance Team at Trail of Bits

Suha Sabi Hussain is a security engineer on the machine learning assurance team at Trail of Bits. She has worked on projects such as the Hugging Face Safetensors security audit and Fickling. She received her BS in Computer Science from Georgia Tech where she also conducted research at the Institute for Information Security and Privacy. She previously worked at the NYU Center for Cybersecurity and Vengo Labs. She's also a member of the Hack Manhattan makerspace, a practitioner of Brazilian Jiu-Jitsu, and an appreciator of NYC restaurants.

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 12:15-13:15 PDT

Title: Indivisible
When: Saturday, Aug 10, 12:15 - 13:15 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

Arizona Secretary of State Adrian Fontes has been educating election officials about the capabilities of current tools to create synthetic content: GenAI used to create text for advanced spear phish targeting election officials, cloned voices of election officials explaining to their real
counterparts how their voices could be weaponized to confuse staff and poll workers, lastly, high quality deepfakes of Secretary Fontes himself showing how easy it could be to use an elected official's own likeness against them. This presentation will be a deep dive into how we predict GenAI attacks will be used during the 2024 General Election and will provide a framework for the audience, hardening them against
what is coming.

SpeakerBio: Michael Moore

After volunteering to be a poll worker, Michael Moore developed a passion for Election Security. He was the first Information Security Officer for the Maricopa County Recorder's office and is now the first Chief Information Security Officer for the Arizona Secretary of State.Michael believes it is only through effective federal, state, and local government partnerships, as well as assistance from trusted vendors that we can protect our democracy and fulfill our duty to the American voter. The greatest threats to elections are MDM and the resulting insider threat caused by radicalized citizens. The best protection against these threats is combatting lies with the truth, developing secure and resilient systems that prevent attacks whenever possible, allow for detections of compromise and facilitate accurate and rapid recovery. Michael has pushed forward these initiatives in his own organizations as well as across the Michael is an alumnus of Arizona State University with a B.S. in Mathematics and a B.A. in Education,CISSP, Certified Election Official (CEO) and Certified Public Manager (CPM).Elections community.

Return to Index - Add to Google - ics Calendar file

AIxCC - Friday - 16:00-16:45 PDT

Title: Industry Panel: The Modern Evolution of LLMs
When: Friday, Aug 9, 16:00 - 16:45 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

AIxCC Collaborator Panel Discussion

Speakers: Dr. Matt Turek,Heather Adkins,Jason Clinton,Matt Knight,David Weston

SpeakerBio: Dr. Matt Turek, Deputy Office Director for DARPA's Information Innovation Office (I2O) at DARPA

Dr. Matt Turek assumed the role of deputy office director for DARPA's Information Innovation Office (I2O) in May 2022. In this position, he provides technical leadership and works with program managers to envision, create, and transition capabilities that ensure enduring information advantage for the United States and its allies.

Turek joined DARPA in July 2018 as an I2O program manager, and served as acting deputy director of I2O from June 2021 to October 2021. He previously managed the Media Forensics (MediFor), Semantic Forensics (SemaFor), Machine Common Sense (MCS), and Explainable AI (XAI) programs as well as the Reverse Engineering of Deception (RED) AI Exploration program (AIE). His research interests include computer vision, machine learning, artificial intelligence, and their application to problems with significant societal impact.

Prior to his position at DARPA, Turek was at Kitware, Inc., where he led a team developing computer vision technologies. His research focused on multiple areas, including large scale behavior recognition and modeling; object detection and tracking; activity recognition; normalcy modeling and anomaly detection; and image indexing and retrieval. Turek has made significant contributions to multiple DARPA and Air Force Research Lab (AFRL) efforts and has transitioned large scale systems for operational use. Before joining Kitware, Turek worked for GE Global Research, conducting research in medical imaging and industrial inspection.

Turek holds a doctorate of philosophy in computer science from Rensselaer Polytechnic Institute, a Master of Science in electrical engineering from Marquette University, and a Bachelor of Science in electrical engineering from Clarkson University. His doctoral work focused on combinatorial optimization techniques for computer vision problems. Turek is a co-inventor on several patents and co-author of multiple publications, primarily in computer vision.

SpeakerBio: Heather Adkins, Vice President of Security Engineering at Google

Heather Adkins is a 22-year Google veteran and founding member of the Google Security Team. As head of Google’s Office of Cybersecurity Resilience she leads the efforts to maintain the safety and security of Google’s networks, systems and applications, and represents Google in government and industry forums globally. As deputy chair of CISA’s Cyber Safety Review Board, she works to isolate the root causes of major security incidents impacting national security and make recommendations to policy-makers, standards bodies, and industry on improving the safety posture of modern computing. She is co-author of Building Secure and Reliable Systems (O’Reilly, 2020), is sought out to speak at high-profile conferences, and serves on the BlackHat review board. Heather advises numerous organizations on how to adopt modern defendable architectures, is a strategic advisor for a number of publicly-traded cybersecurity companies, and is a member of the steering committee for the IST Ransomware Taskforce. She is passionate about election security and was a senior advisor on the Defending Digital Democracy project at the Harvard Kennedy School’s Belfer Center.

Heather Adkins, a seasoned cybersecurity expert with over two decades at Google, is a founding member of the Google Security Team. Currently heading Google's Office of Cybersecurity Resilience, she safeguards Google's vast digital infrastructure and represents the company in global technology and policy forums. Her influence extends to national security, as deputy chair of CISA's Cyber Safety Review Board, where she analyzes major security incidents and makes

recommendations for policy-makers, standards bodies and industry. A recognized thought leader, Heather co-authored Building Secure and Reliable Systems (O'Reilly, 2020), is a sought-after speaker at major conferences, and serves on the BlackHat review board. She advises numerous organizations on modern security practices, including publicly-traded cybersecurity companies and as a member of the steering committee for the IST Ransomware Taskforce. A passionate advocate for election security, Heather served as a senior advisor on the Defending Digital Democracy project at Harvard's Kennedy School.

SpeakerBio: Jason Clinton, Chief Information Security Officer at Anthropic

Jason is Chief Information Security Officer at Anthropic. Previously, he led Chrome Infrastructure Security at Google. Earlier work includes ChromeOS build integrity, Android Pay security, digital coupons, beowulf computing, and secure thin clients. He's the author of Ruby Phrasebook and contributed to the GNOME project.

SpeakerBio: Matt Knight, Head of Security at OpenAI
No BIO available

SpeakerBio: David Weston, Microsoft
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 15:00-16:59 PDT

Title: Injecting and Detecting Backdoors in Code Completion Models
When: Saturday, Aug 10, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Classroom - Map

Description:

Immerse yourself in a workshop where we guide participants in creating a covert trojan within code completion models. Learn to inject a backdoor discreetly, then explore detection techniques. Gain hands-on experience crafting and identifying hidden threats, unveiling the underbelly of trusted coding.

Speakers:Ori Ron,Tal Folkman

SpeakerBio: Ori Ron

Ori Ron, an experienced Application Security Researcher at Checkmarx, joined the company in 2016. With over eight years of expertise in the field, Ori specializes in identifying and mitigating security vulnerabilities in software systems. His research spans the application security aspects of many programming languages, technologies, and environments.

SpeakerBio: Tal Folkman

Tal brings over 7 years of experience to her role as a supply chain security research team lead within Checkmarx Supply Chain Security group. She is in charge of detecting tracking and stopping Opensource attacks.

Return to Index - Add to Google - ics Calendar file

Title: Insert coin: Hacking arcades for fun
When: Saturday, Aug 10, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

Since we were children we wanted to go to the arcade and play for hours and hours for free. How about we do it now? In this talk I'm gonna show you some vulnerabilities that I discovered in the cashless system of one of the biggest companies in the world, with over 2,300 installations across 70 countries, from arcades in Brazil, amusement parks in the United Arab Emirates to a famous roller coaster in Las Vegas. We will talk about API security, access control and NFC among other things.

Description

The talk is divided into 10(+1) stages. Starting at Stage 0, I will relate the origin of the idea during H2HC Brazil in 2023. Initially, the proposal was an arcade in Brazil with a debit card system.

In Stage 1, I will present the company, the NFC card, an application to charge money and check our data, but without exploitable vulnerabilities due to the use of middleware.

In the next stage, the focus shifts to the company responsible for the debit card system. This Argentine company dominates the market, with more than 2300 installations in 70 countries, ranging from arcades to a famous roller coaster in Las Vegas. During the investigation, the /api endpoint on the server was identified, filtering out endpoints that did not return 404 or 200. DNS enumeration and the use of Shodan revealed an outdated info.php, as well as other servers with open ports and versions with vulnerabilities. Documentation was also found in /api/v2 without the necessary credentials.

In Stage 3, the IDOR and Broken Authentication vulnerabilities will be explained. Then I will present endpoints in the system that allow us to exploit these vulnerabilities and obtain card information and personal customer data.

Then, it will be revealed that the company provides a mobile application. When decompiling some applications, keys and API endpoints were discovered. All APKs were similar, differing only in keys and endpoints. Now, with these credentials we have the ability to recharge credit to our debit card.

In Stage 5, we will explain the Account Takeover attack and how to execute it on the system via API. Also I'll explain Race Condition found in the API.

In the next scenario, a server found in Shodan: The online event booking system. Confidential information was found here, such as all Argentinean invoices, logs and extra company information, obtained by script written by me.

A reservation management portal was also identified with a Broken Access Control vulnerability, allowing us to view and modify all reservations, including modifying prices. It is important to note that all of these vulnerabilities affect ALL of the company's customers.

As we near the end, other servers will be quickly highlighted, such as the company's public Zendesk, allowing user creation and access to useful information. A U.S. case will be presented where a go-karting facility uses this system, allowing access to all monitors. Other examples include an amusement park company in Spain providing links to their park management consoles, and similar findings in Chile, Ecuador and Phoenix.

The last scenario will explain the NFC system, focusing on card reading and manipulation due to lack of security. Some attacks, such as changing the ID and referencing another card, will be shown. I'm also going to show the "feature" of emulating the card with the NFC of android phones, thus being able to emulate any card.

The idea of the talk is to demonstrate that even in 2024 there are significant systems with many users and with "basic" vulnerabilities known for years. Also I would like to encourage new generations to do ethical hacking and help generate a good relationship between hackers and companies. Computer security education and training are crucial to prevent attacks and protect our digital assets.

Outline

- Stage 0
  - Introduction
- Stage 1
  - About Brazilian arcade and cashless system
  - NFC Card
  - Website to charge money and view data
- Stage 2
  - Company who provide the system
  - More than 2300 installations across 70 countries
  - Api endpoints
- Stage 3
  - IDOR and Broken Authentication
  - A lot of user and cards data
  - Not just arcades. Roller coaster Vegas. Clients around the world
- Stage 4
  - Mobile app for all the customers
  - Keys and endpoints in plain text (DEMO)
  - Endpoint to recharge credits
- Stage 5
  - Account Takeover (DEMO)
  - Race Condition (DEMO)
- Stage 6
  - Online Party Booking
  - A lot of confidential information
  - Script to get data (DEMO)
- Stage 7: Booking Management portal
  - Broken Access Control
  - List and modify all the bookings
- Stage 8: Side servers
  - Public zendesk with data
  - Go-karting in U.S.
  - Amusement park in Spain
  - Chile, Ecuador, Phoenix
- Stage 9: NFC
  - Brazilian card
  - Leak security
  - Android NFC
- Stage 10
  - A lot of customers in the U.S.
  - Conclusions
  - QA

SpeakerBio: Ignacio Daniel Navarro, Appication security / Ethical hacker

Ignacio Navarro, an Ethical Hacker and Security Researcher from Cordoba, Argentina. With around 6 years in the cybersecurity game, he's currently working as an Application Security. Their interests include code analysis, web application security, and cloud security.

Speaker at Hackers2Hackers, Security Fest, BSides, Diana Initiative, Hacktivity Budapest, 8.8, Ekoparty.

Return to Index - Add to Google - ics Calendar file

Title: Inside Dash Cam: Custom Protocols and Discovered 0-days
When: Friday, Aug 9, 17:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

In recent years, the use of dash cams has surged, making them an essential component of modern vehicles. To enhance user convenience, many dash cams are now equipped with network connectivity. This growth in the dash cam market has heightened the importance of vehicle and personal data security. However, network-connected dash cams pose potential security risks to their availability and key functionalities. In this presentation, we will comprehensively analyze dash cams from various countries, including South Korea, the USA, Germany, and China, as well as built-in dash cams. During our analysis, we discovered numerous zero-day vulnerabilities (such as OS Command Injection, Logical Bugs, and insufficient authentication) that pose significant security threats. Vulnerabilities were primarily found during the dash cam boot process, configuration changes, and communications via custom protocols.

We will detail the dash cam analysis process in the following sequence: - [Analysis Process] - Acquiring firmware through official websites or apps - Extracting the file system to analyze the initial boot logic - Analyzing the boot logic to identify vulnerabilities or debugging ports to gain shell access - Utilizing the obtained shell for remote debugging of the main system

Interestingly, our analysis of 10 different dash cams revealed that 4 devices used the same OEM board from a common manufacturer. These 4 devices shared similar vulnerabilities, and exploiting a vulnerability found in one device allowed us to successfully exploit all of them. Our research uncovered common security vulnerabilities across multiple dash cams, and we will discuss measures to prevent these vulnerabilities. We will particularly focus on analyzing the custom protocols used by dash cams and the security risks associated with them. This presentation aims to raise awareness of potential security threats in dash cams and encourage manufacturers to produce more secure products. We hope to drive industry standards and best practices to ensure the safety and security of these increasingly critical devices. By sharing our findings, we aim to highlight the importance of dash cam security and provide insights that can lead to more secure designs and implementations.

Speakers: Hyo Jin Lee,Hanryeol Park

SpeakerBio: Hyo Jin Lee, Senior Researcher, R&D Team at ZIEN

Senior Researcher HYOJIN LEE, R&D Team, IoT Security Company ZIEN

- Helped hundreds of companies fix security vulnerabilities, including LG, EY, Korea Investment & Securities, KOREA ELECTRONICS ASSOCIATION, etc
- Operated booth and presented at the Korea Security Conference SECON (2024)
- Operated booth at RSAC (2024)
- First place in the Korea Home IoT Challenge (Cyber Security Challenge 2022)
- Fourth place in the Korea Smart City Challenge (Cyber Security Challenge 2023)
- Recipient of the "Excellence in Cybersecurity Award" from the Ministry of SMEs and Startups (MSS) at the Korea Security Conference WACON 2023
- Holder of five Korean patents, including one related to IoT collection modules.

SpeakerBio: Hanryeol Park, Senior Researcher at ZIEN Lab
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 13:00-13:45 PDT

Title: Inside the FBI's Secret Encrypted Phone Company 'Anom'
When: Saturday, Aug 10, 13:00 - 13:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

In 2018, a secure communications app called Anom started to gain popularity among organized criminals. Soon, top tier drug traffickers were using it all over the world. Because they thought their messages were secure, smugglers and hitmen coordinated high stakes crimes across the platform. But Anom had a secret: it was secretly run by the FBI.

For years Joseph Cox has investigated the inside story of Anom, speaking to people who coded the app, those who sold it, criminals who chatted across it, and the FBI agents who surreptitiously managed it. This new talk, building on details from his recent book DARK WIRE, will include never-before-published technical details on how the Anom network functioned, how the backdoor itself worked, and how Anom grew to such a size that the FBI started to lose control of its own creation.

It will also reflect on how police have entered a new phase of compromising entire encrypted phone networks, with little to no debate from the public, and provide critical insight on what really happens when authorities introduce a backdoor into a telecommunications product.

DARK WIRE: The Incredible True Story of the Largest Sting Operation Ever, June 4th, 2024: link

SpeakerBio: Joseph Cox, Co-Founder at 404 Media

Joseph Cox is an investigative journalist and author of DARK WIRE, the inside story of how the FBI secretly ran its own encrypted phone company called Anom to wiretap the world. He produced a series of exclusive articles on Anom for VICE's Motherboard, and is now a co-founder of 404 Media.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis

When: Friday, Aug 9, 10:00 - 17:59 PDT

Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Learn the trade secrets of elite embedded security researchers and exploit developers. This hands-on workshop equips you with the QEMU and GDB skills needed to emulate and debug embedded system processes.

Friday, August 9th / Saturday, August 10th

```
10:00 am - QEMU Primer
11:00 am - QEMU Emulation
2:00 pm - Debugging with QEMU and GDB
3:00 pm - Q&A for Workshops
```

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis

When: Saturday, Aug 10, 10:00 - 17:59 PDT

Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Learn the trade secrets of elite embedded security researchers and exploit developers. This hands-on workshop equips you with the QEMU and GDB skills needed to emulate and debug embedded system processes.

Friday, August 9th / Saturday, August 10th

```
10:00 am - QEMU Primer
11:00 am - QEMU Emulation
2:00 pm - Debugging with QEMU and GDB
3:00 pm - Q&A for Workshops
```

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Inside the Toolkit of Elite Embedded Security Experts - Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis

When: Sunday, Aug 11, 10:00 - 12:59 PDT

Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Learn the trade secrets of elite embedded security researchers and exploit developers. This hands-on workshop equips you with the QEMU and GDB skills needed to emulate and debug embedded system processes.

Friday, August 9th / Saturday, August 10th

```
10:00 am - QEMU Primer
11:00 am - QEMU Emulation
2:00 pm - Debugging with QEMU and GDB
3:00 pm - Q&A for Workshops
```

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 15:30-16:30 PDT

Title: Intermediate Physical Security
When: Saturday, Aug 10, 15:30 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Physical Red Teams are the most dynamic, exciting, and fast paced engagements we can perform. It requires good decision making under pressure and intimate knowledge of a vast landscape of physical security mechanisms. This talk equips you with the knowledge of over a dozen techniques I use on engagements, delivering the most effective lessons from both lab work and field work. In one action packed hour we'll cover top bypasses for padlocks, doors, RFID systems and more.

SpeakerBio: Justin Wynn, Director of the Red Team at Coalfire

Justin Wynn is the Director of the Red Team at Coalfire and is a Physical Security SME. He's broken into nearly every type of building: data centers, banks, courthouses - you may be familiar with his wrongful arrest in the latter. He's a keynote speaker who has conducted over 350 penetration tests and physical engagements. His pastimes include bank robbing, algorithmic option trading, public speaking, community development, and world peace by founding the militant wing of the Salvation Army.

Return to Index - Add to Google - ics Calendar file

RCV - Saturday - 10:00-10:59 PDT

Title: Interview - CATO Networks, Hosted by Dhruv Shah
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This is an AMA/Podcast that will be recorded on-site.

Speakers:CATO Networks,Dhruv Shah

SpeakerBio: CATO Networks
No BIO available
SpeakerBio: Dhruv Shah
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Saturday - 12:00-12:59 PDT

Title: Interview - Daniel Miessler, Hosted by Ankur
When: Saturday, Aug 10, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This is an AMA/Podcast that will be recorded on-site.

Speakers: Daniel Miessler,Ankur

SpeakerBio: Daniel Miessler
No BIO available
SpeakerBio: Ankur
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 13:00-13:59 PDT

Title: Interview - Mika Devonshire, Hosted by Himanshu Das
When: Friday, Aug 9, 13:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This is an AMA/Podcast that will be recorded on-site.

Speakers: Mika Devonshire,Himanshu Das

SpeakerBio: Mika Devonshire
No BIO available
SpeakerBio: Himanshu Das
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Saturday - 11:00-11:59 PDT

Title: Interview - RedHunt Labs (Kunal), Hosted by Anant Shrivastava
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This is an AMA/Podcast that will be recorded on-site.

Speakers: RedHunt Labs (Kunal),Anant Shrivastava

SpeakerBio: RedHunt Labs (Kunal)
No BIO available
SpeakerBio: Anant Shrivastava
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 15:00-15:59 PDT

Title: Interview - Scott Helme, Hosted by Shubham
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This is an AMA/Podcast that will be recorded on-site.

Speakers: Scott Helme,Shubham

SpeakerBio: Scott Helme
No BIO available
SpeakerBio: Shubham
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 16:00-16:59 PDT

Title: Interview - the gumshoo, Hosted by Ram
When: Friday, Aug 9, 16:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This is an AMA/Podcast that will be recorded on-site.

Speakers:the gumshoo,Ram

SpeakerBio: the gumshoo
No BIO available
SpeakerBio: Ram
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 21:00-01:59 PDT

Title: Intigriti Hack Shack
When: Saturday, Aug 10, 21:00 - 01:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Join us at the Hack Shack Saturday night from 21: 00-02:00 in room 208 for an evening full of exploits and fun! Enjoy some byte-sized bites, groove to our cyber beats, and mingle with the best in the bug bounty biz. Stop by Intigriti's booth in Exhibitors area before the party and grab a scratch card for your chance to win a free drink! Don't miss out on this bug bounty bonanza!

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-10:59 PDT

Title: Intro to Circuit Python (Badge class level 1) (Overflow if Friday is too full)
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

(NOTE: This is an overflow class only if the first session is full)

Learn how to program the DCNextGen Badge

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 11:00-11:59 PDT

Title: Intro to Circuit Python (Badge class level 1)
When: Friday, Aug 9, 11:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Learn how to program the DCNextGen Badge

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 10:00-10:59 PDT

Title: Intro to QKD: Quantum Key Exchange: Beyond the Hype
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Quantum Key Distribution (QKD) has been heralded as the future of secure communications, but what does it really offer, and how does it work? This talk is a deep dive into the physics that underpins QKD, tailored for the technically curious and sceptical minds at DefCon. We'll explore the foundational principles of quantum mechanics that make QKD possible, with a focus on the BB84 protocol and Continuous Variable QKD (CV-QKD). Additionally, we'll compare these quantum methods with classical key exchange techniques, discussing their strengths and limitations in real-world applications—without the hype. Whether you're a seasoned cryptographer or new to the field, this session will provide a practical and clear-eyed understanding of quantum key exchange.

SpeakerBio: Ben Varcoe
No BIO available

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 10:05-11:25 PDT

Title: Intro to Quantum with Q#
When: Friday, Aug 9, 10:05 - 11:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Quantum computing harnesses the laws of nature to solve problems that are infeasible on conventional computers, such as integer factorization, which has applications in cryptography, or analyzing properties of molecules and chemical reactions.

In this workshop, you will learn the basics of quantum computing and quantum programming using Q# programming language and Azure Quantum Development Kit. You will learn enough to write your first quantum programs — quantum random number generator and Deutsch-Jozsa algorithm — an algorithm that is exponentially faster than any deterministic classical algorithm for that problem. HINT - for those looking to compete in the Quantum CTF, Mariia's talk will be very useful indeed!!

SpeakerBio: Mariia Mykhailova

Mariia Mykhailova is a principal quantum software engineer at Microsoft Quantum. She has been part of the team since early 2017, joining just in time to participate in the development of the first version of the quantum programming language that became Q#. She works on developing software for fault-tolerant quantum computation, as well as quantum education and outreach for Azure Quantum Development Kit. Mariia is the author and maintainer of the Quantum Katas project – an open-source collection of hands-on tutorials and programming problems for learning quantum computing. She is also a part-time lecturer at Northeastern University, teaching "Introduction to Quantum Computing" since 2020, and the author of the O'Reilly book "Q# Pocket Guide" and the upcoming Manning book "Quantum Programming in Depth".

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 12:30-13:30 PDT

Title: Introduction to Creating Osquery Extensions: Enhancing Endpoint Security Visibility
When: Saturday, Aug 10, 12:30 - 13:30 PDT
Where: LVCC West/Floor 3/W309 - Map

Description:

This workshop offers a hands-on introduction to developing Osquery extensions for Linux and macOS, aimed at beginners seeking to enhance endpoint security visibility. Through guided instruction, participants will explore Osquery extension architecture, the Thrift API, SQL-based querying, and module integration. Real-world examples and best practices will be emphasized, providing attendees with the skills to create custom extensions tailored to organizational security needs. By the end of the session, participants will have the confidence to leverage Osquery effectively in bolstering endpoint security defenses. Python will be used during the workshop. Basic knowledge of python will be sufficient to follow workshop.

Outline:

- Introduction to Osquery and its role in endpoint security
- Overview of Osquery extension architecture
- First extension
- Understanding the basics of Osquery Thrift API
- Real-world examples and use cases
- Hands-on exercises and practical application
- Q&A and interactive discussion

Join us for a comprehensive introduction to developing Osquery extensions tailored for Linux and macOS environments. This hands-on training session, designed for beginners, will demystify the process of extending Osquery functionalities, empowering attendees to bolster their endpoint security strategies. Throughout the workshop, participants will learn the fundamentals of Osquery extension development, gain practical insights through real-world examples, and discover how to leverage Osquery's capabilities to enhance visibility into their endpoint ecosystems. By the end of this session, attendees will have the confidence and knowledge to create custom Osquery extensions, effectively enriching their organization's security posture.

SpeakerBio: Kivanc Aydin

With a distinguished career spanning multiple sectors, Kivanc is a seasoned cybersecurity expert with a rich background in detection, monitoring, and incident response. Kivanc began their professional journey in the military, where they honed their skills in cyber defense and security strategies. Transitioning from military service, they brought their expertise to academia, delivering lectures at the university level and sharing their deep knowledge with the next generation of cybersecurity professionals.

Currently, Kivanc is making significant contributions to the payment industry, where they apply their extensive experience to safeguard critical financial infrastructures. Their focus remains on enhancing detection and response capabilities to address emerging cyber threats effectively.

In addition to practical experience, Kivanc holds a Master's degree in Cyber Security and multiple industry-standard certifications, underscoring their commitment to excellence and professional development. A strong advocate for open-source solutions, they actively contribute to and utilize open-source tools to drive innovation and community collaboration within the cybersecurity landscape.

Driven by a passion for continuous learning and knowledge sharing, Kivanc is dedicated to empowering others through education and mentorship, believing that collective effort is key to advancing the field of cybersecurity.

ASV - Saturday - 10:30-11:30 PDT

Title: Introduction to Drone Security
When: Saturday, Aug 10, 10:30 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

Recent advancements in drone technology are opening new opportunities and applications in various industries across all domains. Drones are quickly becoming integrated into our everyday lives for commercial and recreational use like many IoT devices; however, these advancements also present new cybersecurity challenges as drones grow in popularity. This talk provides an introduction to drone security covering the core components of drone technology (e.g., hardware, software, firmware, and communication protocols), cybersecurity risks and mitigations, and cybersecurity best practices for drone operations. Attendees will gain an understanding of drone systems and important security measures that help protect these devices (and its operators) from emerging and evolving threats.

SpeakerBio: Hahna Kane Latonick

For the past 18 years of her engineering career, Hahna Kane Latonick has worked throughout the defense industry specializing in cybersecurity as a computer security researcher for the Department of Defense and other defense contracting companies. She has been featured as a cybersecurity subject matter expert on Fox Business News, ABC, U.S. News and World Report, and other national media outlets. She currently serves as a Director of Security Research for a cybersecurity firm and has led four tech startups related to computer security, serving as CTO of two of them, VP of R&D, and Director of R&D. She has trained and developed security researchers at one of the top five aerospace and defense industry companies. She has also taught at Black Hat, CanSecWest, Ringzer0, and the Security BSides Orlando conferences. At the 2023 DEF CON IoT CTF, she and her team tied for first place. In 2014, she became a DEFCON CTF finalist, placing in 6th and ranking in the top 1.5% of ethical hackers worldwide. She also holds security certifications, including CISSP, CEH, and Certified Android Exploit Developer. Latonick attended Swarthmore College and Drexel University where she earned her B.S. and M.S. in Computer Engineering along with a Mathematics minor.

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 11:00-11:30 PDT

Title: Introduction to IPv6
When: Saturday, Aug 10, 11:00 - 11:30 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Most of the Internet today is running on a legacy version of the Internet Protocol: IPv4. Despite of this, the number of engineers, especially in security, who know how to use IPv6 is relatively low. In this talk we take you through why today's Internet does not live up to its original vision, take you back to the past to show you what the IPv4 Internet used to look like, and, through this, reveal the secrets that will allow you finally understand IPv6.

SpeakerBio: Denis Smajlović, Nova

With a background in security consulting, having worked for some of the largest financial institutions in Scandinavia, and biggest tech companies in the Bay Area, Denis started Nova to provide web application, network penetration testing, and bug bounty triage services at a scale that enables a greater focus on the specific needs of each individual client.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 15:00-15:50 PDT

Title: Introduction to Kubernetes common attack techniques
When: Saturday, Aug 10, 15:00 - 15:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

Kubernetes is the de facto operating system of the cloud, and more and more organizations are running their workloads on Kubernetes. While Kubernetes offers many benefits, it also introduces new security risks, such as cluster misconfiguration, leaked credentials, cryptojacking, container escapes, and vulnerable clusters.

This workshop will teach you the fundamentals of Kubernetes security, you'll learn how to exploit workloads running on a Kubernetes environment using Living Off the Land (LotL) techniques like exploiting Insecure APIs, Secrets Theft, Container Escape and Pod Privilege Escalation, similar to the ones used by real-world threat actors.

SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 13:00-14:59 PDT

Title: Introduction to MITRE Caldera Through Adversary Emulation
When: Friday, Aug 9, 13:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

MITRE Caldera is a scalable, automated adversary emulation, open-source cybersecurity platform developed by MITRE. It empowers cyber practitioners to save time, money, and energy through automated security assessments. Caldera not only tests and evaluates detection/analytic and response platforms, but it also provides the capability for your red team to perform manual assessments with computer assistance. This is achieved by augmenting existing offensive toolsets. The framework can be extended to integrate with any custom tools you may have. The development team behind the platform is a group of red teamers, software developers, exploit writers, cyber threat analysts, AI researchers, cybersecurity engineers, and computer scientists. They all pursue the common goal of building a premier adversary emulation platform for our security defenders around the world. To showcase Caldera at DEF CON 32, we will present a scenario that a commercial or corporate entity may ask of a security team. In this scenario, a concerned organization is requesting a security team to develop a repeatable adversary emulation plan based on current cyber threat intelligence (CTI) for a specific advanced persistent threat (APT) that has been targeting the organization's industry sector. We will create three cyber threat intelligence reports for this adversary detailing the tactics, techniques, and procedures (TTPs) attributed to them. These TTPs will correspond with the abilities available in Caldera's Stockpile and Atomic plugins. This collection of abilities makes the job of developing an adversary emulation very simple. We will go on to demonstrate how to develop an adversary emulation plan in Caldera utilizing the relevant TTPs described in the CTI reporting. Finally, we will execute the new adversary emulation plan against the target machines and display the facts that Caldera collects during an operation, the outputs of all commands run, and the final report generated by the Debrief plugin.

Speakers:
Rachel Murphy,Mark Perry

SpeakerBio:
Rachel Murphy, Cyber Security Engineer at MITRE Corp

Rachel Murphy is a Cyber Security Engineer at MITRE Corp. She has a B.S. in Mechanical Engineering and prior to joining MITRE, she worked as a mechanical engineer at NASA performing thermal analysis for the International Space Station at Johnson Space Center in Houston, TX. Rachel has worked on projects in adversary emulation, red teaming, cyber threat intelligence, and software development. Part of this work includes supporting Caldera's research in artificial intelligence, developing Caldera workshops like this one, and promoting Caldera's benefactor program. She has also served as a red team operator for MITRE Engenuity's ATT&CK Evaluations.

SpeakerBio:
Mark Perry, Lead Applied Cyber Security Engineer at MITRE Corp

Mark Perry is a Lead Applied Cyber Security Engineer at MITRE Corp, where he specializes in adversary emulation and work development. With a robust background in infrastructure and cyber security frameworks, Mark brings extensive expertise to his role, focusing on fortifying systems against sophisticated cyber threats. He has worked on projects involving adversary emulation, red teaming, cyber threat intelligence, and software development. Mark also leads development and delivery of Caldera workshops, providing participants with practical, hands-on training utilizing cybersecurity techniques. Additionally, he actively promotes Caldera's benefactor program, fostering community support and engagement to further the development of cybersecurity tools and resources. Outside of his professional endeavors, Mark enjoys traveling and is a supercar enthusiast.

Return to Index - Add to Google - ics Calendar file

PYV - Saturday - 10:15-10:20 PDT

Title: Introduction to Payment Village CTF
When: Saturday, Aug 10, 10:15 - 10:20 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

Find out how to participate in the Payment Village CTF

SpeakerBio: Leigh-Anne Galloway, Director of Research at UNDERLE LTD

Leigh-Anne Galloway is the Payment Village Lead and Director of Research at UNDERLE LTD. Leigh-Anne started her career in incident response, leading investigations into payment card data breaches. This is where she discovered her passion for security advisory and payment technologies. She authored research on ATM security, application security and payment technology vulnerabilities; and has previously spoken at DevSecCon, BSides, Hacktivity, 8dot8, OWASP, and Troopers, Black Hat USA, Black Hat Europe and DEF CON. She also serves on the board for Black Hat Europe.

Return to Index - Add to Google - ics Calendar file

PYV - Friday - 10:15-10:20 PDT

Title: Introduction to Payment Village CTF
When: Friday, Aug 9, 10:15 - 10:20 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

Find out how to participate in the Payment Village CTF

SpeakerBio: Leigh-Anne Galloway, Director of Research at UNDERLE LTD

Leigh-Anne Galloway is the Payment Village Lead and Director of Research at UNDERLE LTD. Leigh-Anne started her career in incident response, leading investigations into payment card data breaches. This is where she discovered her passion for security advisory and payment technologies. She authored research on ATM security, application security and payment technology vulnerabilities; and has previously spoken at DevSecCon, BSides, Hacktivity, 8dot8, OWASP, and Troopers, Black Hat USA, Black Hat Europe and DEF CON. She also serves on the board for Black Hat Europe.

Return to Index - Add to Google - ics Calendar file

PYV - Saturday - 10:45-10:59 PDT

Title: Introduction to the Payment Village badge
When: Saturday, Aug 10, 10:45 - 10:59 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

In this workshop you will learn how to assemble and use the village badge, and how it can be used to solve challenges in the CTF

SpeakerBio: Leigh-Anne Galloway, Director of Research at UNDERLE LTD

Leigh-Anne Galloway is the Payment Village Lead and Director of Research at UNDERLE LTD. Leigh-Anne started her career in incident response, leading investigations into payment card data breaches. This is where she discovered her passion for security advisory and payment technologies. She authored research on ATM security, application security and payment technology vulnerabilities; and has previously spoken at DevSecCon, BSides, Hacktivity, 8dot8, OWASP, and Troopers, Black Hat USA, Black Hat Europe and DEF CON. She also serves on the board for Black Hat Europe.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 11:30-11:55 PDT

Title: Invisible Invaders: Strategies to Combat Living Off the Land Techniques in ICS
When: Friday, Aug 9, 11:30 - 11:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

While living off the land attacks have always been possible in industrial environments, a notable uptick has been reported recently between Volt Typhoon's five-plus year campaign and reports of attackers using unauthenticated industrial protocols to manipulate and impact industrial processes. This talk will explore past living off the land attacks in industrial environments, the differences in IT and OT living off the land attacks, and provide approaches to counter these attacks.

SpeakerBio: Dan Gunter, Founder and CEO at Insane Cyber

Dan Gunter is the founder and CEO of Insane Cyber, a San Antonio, Texas-based technology company that provides a cybersecurity automation platform for forward, at at-home investigations supporting critical operations, as well as tailored proactive and reactive services. Prior to Insane Cyber, Dan was an early employee at Dragos, an industrial cybersecurity startup, where he established and served as Director of Research and Development and as one of the first principal analysts executing and advising on threat hunting in power, oil & gas, mining, and other critical infrastructure environments. Before Dragos, Dan served as an officer in the United States Air Force with a variety of offensive and defensive roles across the Department of Defense.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:15-11:45 PDT

Title: IoT Cat Lamp
When: Friday, Aug 9, 10:15 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Want to create a cute, squishy, Wi-Fi controllable LED cat lamp? In this workshop, we'll create a cute cat lamp featuring programmable IoT LED's, giving it custom light animations and Wi-Fi control! Your adorable cat lamp can be controlled over Wi-Fi with WLED, allowing you to control it with home automation software. You will create open source, Wi-Fi controlled LED art; learn basic soldering; and take home the remote-controlled Pusheen lamp of your dreams.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 12:00-13:30 PDT

Title: IoT Cat Lamp
When: Sunday, Aug 11, 12:00 - 13:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Want to create a cute, squishy, Wi-Fi controllable LED cat lamp? In this workshop, we'll create a cute cat lamp featuring programmable IoT LED's, giving it custom light animations and Wi-Fi control! Your adorable cat lamp can be controlled over Wi-Fi with WLED, allowing you to control it with home automation software. You will create open source, Wi-Fi controlled LED art; learn basic soldering; and take home the remote-controlled Pusheen lamp of your dreams.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: IoT Security at DEF CON 32
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Join Finite State live on the Tech Done Different Podcast live at 2: 30 on the 9th with host Ted Harrington. Finite State and ISE will be discussing all things DEF CON 32 and the state of IoT security. This will be a live recording!

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: IoT Security at DEF CON 32
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Join Finite State live on the Tech Done Different Podcast live at 2: 30 on the 9th with host Ted Harrington. Finite State and ISE will be discussing all things DEF CON 32 and the state of IoT security. This will be a live recording!

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: IoT Security at DEF CON 32
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Join Finite State live on the Tech Done Different Podcast live at 2: 30 on the 9th with host Ted Harrington. Finite State and ISE will be discussing all things DEF CON 32 and the state of IoT security. This will be a live recording!

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: IoT Village CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

The IoT village pi eating contest is a challenge where participants put their hardwear hacking experience to the test by going head to head with other hackers. Participants will be provided all the tooling necessary to get a root shell on an IoT device. Whoever roots the device in the shortest time wins.

In this brand new challenge, participants put their hardware hacking experience to the test by going head to head with other hackers. Participants will be provided all the tooling necessary to get a root shell on an IoT device. Whoever roots the device in the shortest time wins!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: IoT Village CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

The IoT village pi eating contest is a challenge where participants put their hardwear hacking experience to the test by going head to head with other hackers. Participants will be provided all the tooling necessary to get a root shell on an IoT device. Whoever roots the device in the shortest time wins.

In this brand new challenge, participants put their hardware hacking experience to the test by going head to head with other hackers. Participants will be provided all the tooling necessary to get a root shell on an IoT device. Whoever roots the device in the shortest time wins!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: IoT Village CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

The IoT village pi eating contest is a challenge where participants put their hardwear hacking experience to the test by going head to head with other hackers. Participants will be provided all the tooling necessary to get a root shell on an IoT device. Whoever roots the device in the shortest time wins.

In this brand new challenge, participants put their hardware hacking experience to the test by going head to head with other hackers. Participants will be provided all the tooling necessary to get a root shell on an IoT device. Whoever roots the device in the shortest time wins!

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: IoT Village Hacking Playground
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

The IoT Village Hacking Playground is a set of hands-on labs developed to teach the tools and techniques for discovering and exploiting some of the common weaknesses found in IoT devices in just a few minutes. Work at your own pace following our IoT Hacking guides and if you get stuck, our instructors are on hand to provide assistance and answer any questions.

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: IoT Village Hacking Playground
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

The IoT Village Hacking Playground is a set of hands-on labs developed to teach the tools and techniques for discovering and exploiting some of the common weaknesses found in IoT devices in just a few minutes. Work at your own pace following our IoT Hacking guides and if you get stuck, our instructors are on hand to provide assistance and answer any questions.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: IoT Village Hacking Playground
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

The IoT Village Hacking Playground is a set of hands-on labs developed to teach the tools and techniques for discovering and exploiting some of the common weaknesses found in IoT devices in just a few minutes. Work at your own pace following our IoT Hacking guides and if you get stuck, our instructors are on hand to provide assistance and answer any questions.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 11:00-11:50 PDT

Title: Island Hoping: Move from LOLBins to Living off Langs
When: Saturday, Aug 10, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

What keeps me up at night? Is it that I can't break in anymore, or is it that we haven't figured out all the ways to break in? Over the years, we have seen moves to place our applications into smaller attacker surface spaces. We have seen those microservice environments abstract our attack surface. Did we eliminate all attacks? At the same time, we have an explosion of endpoints of applications that run interpreted languages and how those constraints can be broken.

When organisms evolve in the wild, they do so under extreme pressure. Has the pressure to find new ways to get a foothold in environments allowed us to evolve? Attackers are crafty, and defenders have to keep up. This talk demonstrates a methodology and tools for moving from container-constrained environments. They are limited to shells and interpreters. Have you been stuck like this before? Let's get beyond that. How does this tool move beyond containers and constrained environments into Windows and other generic workloads? Let's not worry about LOLBins. Bring your land and get off the air-gapped island.

SpeakerBio: Moses Frost
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 08:15-10:30 PDT

Title: ISSCON
When: Friday, Aug 9, 08:15 - 10:30 PDT
Where: LVCC West/Floor 3/LVCC-L3-Terrace - Map

Description:

Let’s Boop the ISS! Join the Lonely Hackers Club for an extraordinary experience where we’ll use our ham radios to attempt communication with astronauts aboard the International Space Station! We have tracked the orbital passes of the space station and calculated our best chance.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: It's In That Place Where I Put That Thing That Time
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: Other / See Description

Description:

Your friend called. They had their place raided. They swear it's a setup. But now they're in jail and you're the only hope they have. Can you collect the evidence that will let them walk free? Where should you look? The evidence is everywhere, and it could be anywhere. You might be sitting on it. You might be standing near it. It might be stuck to something. It might be lying in plain sight. Find the disks and bring them to us. All they said to you before they hung up was "It's in that place where I put that thing that time." Good luck.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: It's In That Place Where I Put That Thing That Time
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: Other / See Description

Description:

Your friend called. They had their place raided. They swear it's a setup. But now they're in jail and you're the only hope they have. Can you collect the evidence that will let them walk free? Where should you look? The evidence is everywhere, and it could be anywhere. You might be sitting on it. You might be standing near it. It might be stuck to something. It might be lying in plain sight. Find the disks and bring them to us. All they said to you before they hung up was "It's in that place where I put that thing that time." Good luck.

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 21:00-00:59 PDT

Title: Jack Rhysider Masquerade Party
When: Saturday, Aug 10, 21:00 - 00:59 PDT
Where: LVCC West/Floor 3/W325-W326 - Map

Description:

Come party with Jack Rhysider at the Darknet Diaries Masquerade party! You're not going to want to miss this event as there will be free swag, killer music, interactive exhibits, and of course Jack Rhysider.

SpeakerBio: Jack Rhysider
No BIO available

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 10:00-10:30 PDT

Title: Jayson Street - Keynote
When: Saturday, Aug 10, 10:00 - 10:30 PDT
Where: Virtual

Description:

SpeakerBio: Jayson E. Street

Jayson E. Street referred to in the past as:

A "notorious hacker" by FOX25 Boston, "World Class Hacker" by National Geographic Breakthrough Series and described as a "paunchy hacker" by Rolling Stone Magazine. He however prefers if people refer to him simply as a Hacker, Helper & Human.

He's a Simulated Adversary for hire. The author of the "Dissecting the hack: Series" (Which has been taught in colleges and Jayson also appears in college text books as well). Also, the DEF CON Groups Global Ambassador. He's spoken at DEF CON, DEF CON China, GRRCon, DerbyCon and at several other 'CONs & colleges on a variety of Information Security subjects. He was also a guest lecturer for the Beijing Institute of Technology for 10 years.

He loves to explore the world & networks as much as he can. He has successfully robbed banks, hotels, government facilities, Biochemical companies, etc. on five continents (Only successfully robbing the wrong bank in Lebanon once all others he was supposed to)!

Jayson is a highly carbonated speaker who has partaken of Pizza from Bulgaria to Brazil & China to The Canary Islands. He does not expect anybody to still be reading this far but if they are please note he was proud to be chosen as one of Time's persons of the year for 2006.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 10:00-10:30 PDT

Title: Jayson Street - Keynote
When: Saturday, Aug 10, 10:00 - 10:30 PDT
Where: LVCC West/Floor 2/W236 - Map

Description:

SpeakerBio: Jayson E. Street

Jayson E. Street referred to in the past as:

A "notorious hacker" by FOX25 Boston, "World Class Hacker" by National Geographic Breakthrough Series and described as a "paunchy hacker" by Rolling Stone Magazine. He however prefers if people refer to him simply as a Hacker, Helper & Human.

He's a Simulated Adversary for hire. The author of the "Dissecting the hack: Series" (Which has been taught in colleges and Jayson also appears in college text books as well). Also, the DEF CON Groups Global Ambassador. He's spoken at DEF CON, DEF CON China, GRRCon, DerbyCon and at several other 'CONs & colleges on a variety of Information Security subjects. He was also a guest lecturer for the Beijing Institute of Technology for 10 years.

He loves to explore the world & networks as much as he can. He has successfully robbed banks, hotels, government facilities, Biochemical companies, etc. on five continents (Only successfully robbing the wrong bank in Lebanon once all others he was supposed to)!

Jayson is a highly carbonated speaker who has partaken of Pizza from Bulgaria to Brazil & China to The Canary Islands. He does not expect anybody to still be reading this far but if they are please note he was proud to be chosen as one of Time's persons of the year for 2006.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 13:00-13:59 PDT

Title: Jeitinho Cibernético: A Convergência da Segurança no Brasil e América Latina
When: Sunday, Aug 11, 13:00 - 13:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

A convergência entre segurança física e cibernética ainda é pouco explorada em nossa região, muitas vezes devido à dificuldade de acesso a ferramentas específicas. Esta apresentação explora esse conceito e sua importância, ilustrando com casos reais de incidentes que exploraram sistemas de segurança física, detalhando como ocorreram e seus impactos.

Apresentaremos os fundamentos dos sistemas de controle de acesso, abordando arquitetura básica, protocolos de comunicação e tecnologias de credenciais. Em seguida, demonstraremos técnicas práticas de exploração:

- Exploração da interface Wiegand: Mostraremos como explorar essa interface antiga e vulnerável, utilizando a versão DIY do BLE-Key, acessível e econômica.
- Exploração de credenciais vulneráveis: Como iClass Legacy, PROX e MiFare Classic, usando ferramentas como ProxMark3 e Flipper Zero.
- Exploração de credenciais "seguras": Demonstrando ataques de downgrade em credenciais HID Seos com Flipper Zero e um leitor HID Multiclass SE, usando um app desenvolvido por mim como alternativa econômica ao Seader.

SpeakerBio: Ueric Melo, Privacy & Security Awareness Manager, LATAM and Caribbean at Genetec

Meu nome é Ueric Melo, sou Privacy & Security Awareness Manager na Genetec. Atuo ha 27 anos na área de Tecnologia da Informação, e na área de segurança (física e da informação) há mais de 22 anos. Sou formado em processamento de dados e possuo extensão em compliance digital. Já palestrei em diversos eventos no Brasil e America Latinha, a maioria deles focados em profissionais de segurança física e TI.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 14:30-15:15 PDT

Title: Joe and Bruno's Guide to Hacking Time: Regenerating Passwords from RoboForm's Password Generator
When: Friday, Aug 9, 14:30 - 15:15 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

Imagine if you could go back in time to precompute all passwords that could have been generated by an off-the-shelf password generator? With RoboForm versions prior to June 2015, you can!

In Joe and Bruno's Guide to Hacking Time, Joe and Bruno share their story, process, and experiences of reverse engineering RoboForm, finding a weakness in the randomness of the password generation routine, and creating a wrapper to generate all possible passwords that could have been generated within a specific time frame. Their work, using Cheat Engine, Ghidra, x64dbg, and custom code, was done specifically to help someone recover over $3 million of Bitcoin locked in a software wallet, but the attack could be exploited against any account or system protected by a password generated by RoboForm before their 7.9.14 release when this problem was fixed.

- Kung Fury, link
- Cheat Engine
- Ghidra
- x64dbg

Speakers: Joe "Kingpin" Grand,Bruno Krauss

SpeakerBio: Joe "Kingpin" Grand

Joe Grand, also known as Kingpin, is a computer engineer, hardware hacker, teacher, daddy, honorary doctor, occasional YouTuber, creator of the first electronic badges for DEFCON, member of L0pht Heavy Industries, and former technological juvenile delinquent.

SpeakerBio: Bruno Krauss

Bruno Krauss is a software engineer and Bitcoin enthusiast. He demonstrated his knack for password cracking at the age of 13 by bypassing his secondary school's IT security to mine BTC on their PCs and now specializes in cryptocurrency recovery.

Return to Index - Add to Google - ics Calendar file

SEV - Saturday - 10:00-12:30 PDT

Title: John Henry Competition - Human vs. AI & Panel Discussion
When: Saturday, Aug 10, 10:00 - 12:30 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Join us for the thrilling and BRAND NEW competition where professional social engineers battle a cutting-edge AI team to see who can achieve the most objectives, followed by an insightful panel discussion.

Return to Index - Add to Google - ics Calendar file

AIV - Saturday - 10:00-10:59 PDT

Title: Keynote - AI-Powered Cybersecurity: The Importance of Red Teamers
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

As artificial intelligence and machine learning increasingly become the backbone of our cybersecurity infrastructure, we face a new set of ethical challenges that go beyond traditional security concerns. This keynote dives into the critical issues of fairness, transparency, and accountability in AI-driven security systems. We'll explore the relevance of AI ethics to safety and security testing, especially red teaming efforts. Finally, we'll discuss the importance of ethical AI development in cybersecurity, emphasizing the need for diverse development teams, rigorous testing for biases, and ongoing audits of AI systems in production. This keynote aims to spark a crucial conversation in the hacker community about our responsibility to ensure that as we push the boundaries of AI in security, we don't lose sight of the human values and ethical principles that should guide our work.

SpeakerBio: Nikki Pope, NVIDIA
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Keysight CTF Challenge
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Defeat the Keysight CTF challenge for a chance to win a Riscuberry IoT hacking training kit with Riscure Academy online training. See one of the Keysight staff for details. LIGHT THE BEACONS and show us the flag!

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Keysight CTF Challenge
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Defeat the Keysight CTF challenge for a chance to win a Riscuberry IoT hacking training kit with Riscure Academy online training. See one of the Keysight staff for details. LIGHT THE BEACONS and show us the flag!

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Keysight CTF Challenge
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Defeat the Keysight CTF challenge for a chance to win a Riscuberry IoT hacking training kit with Riscure Academy online training. See one of the Keysight staff for details. LIGHT THE BEACONS and show us the flag!

Return to Index - Add to Google - ics Calendar file

CLV - Sunday - 10:35-11:10 PDT

Title: Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access
When: Sunday, Aug 11, 10:35 - 11:10 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

In this talk we will explore vulnerabilities in Amazon Web Services (AWS) products which allowed us to gain access to cloud environments.

Traditionally, adversaries have abused misconfigurations and leaked credentials to gain access to AWS workloads. Things like exposed long-lived access keys and exploiting the privileges of virtual machines have allowed adversaries to breach cloud resources. However, these mistakes are on the customer side of the shared responsibility model. In this session, we will cover vulnerabilities in AWS services that have been fixed and that previously allowed us to access cloud resources.

We will start with an exploration of how Identity and Access Management (IAM) roles establish trust with AWS services. Covering how roles associated with Amazon Cognito and GitHub Actions could be misconfigured to allow anyone in the world to access them. From here, we'll cover a vulnerability we found in AWS Amplify which exposed IAM roles associated with the service to takeover, allowing anyone the ability to assume these roles.

Finally, we will also look at a worst-case scenario: what happens when an attacker finds a confused deputy vulnerability and is able to assume roles in other accounts? Sounds far-fetched? We'll cover a real world example of a vulnerability we found in AWS AppSync that lets us do just that. We'll also discuss how security practitioners can secure their environments, even against a zero-day like this one.

Join us to learn how attackers search for and exploit vulnerabilities in AWS services to gain access to cloud environments.

SpeakerBio: Nick Frichette, Staff Security Researcher at Datadog

Nick Frichette is a Staff Security Researcher at Datadog, where he specializes in offensive AWS security. He is known for finding multiple zero-day vulnerabilities in AWS services and regularly publishing on new attack techniques. In addition to his research, Nick is the creator and primary contributor to Hacking the Cloud, an open source encyclopedia of offensive security capabilities for cloud environments. He is also a part of the AWS Community Builder Program, where he develops content on AWS security.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 12:30-13:15 PDT

Title: Kicking in the Door to the Cloud: Exploiting Cloud Provider Vulnerabilities for Initial Access
When: Friday, Aug 9, 12:30 - 13:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

In this talk we will explore vulnerabilities in Amazon Web Services (AWS) products which allowed us to gain access to cloud environments.

Traditionally, adversaries have abused misconfigurations and leaked credentials to gain access to AWS workloads. Things like exposed long-lived access keys and exploiting the privileges of virtual machines have allowed adversaries to breach cloud resources. However, these mistakes are on the customer side of the shared responsibility model. In this session, we will cover vulnerabilities in AWS services that have been fixed and that previously allowed us to access cloud resources.

We will start with an exploration of how Identity and Access Management (IAM) roles establish trust with AWS services and cover the mechanisms that prevent an adversary from assuming roles in other AWS accounts. We'll then demonstrate a vulnerability that bypassed those protections. We'll cover a real world example of a confused deputy vulnerability we found in AWS AppSync that allowed us to hijack IAM roles in other accounts.

Next, we'll highlight potential misconfigurations involving IAM roles leveraging sts:AssumeRoleWithWebIdentity. These misconfigurations cloud permit unauthorized global access to these roles without the need for authentication, affecting services like Amazon Cognito, GitHub Actions, and more.

Finally, we'll cover a vulnerability we found in AWS Amplify that exposed customer IAM roles associated with the service to takeover, allowing anyone the ability to gain a foothold in that victim account. We'll also discuss how security practitioners can secure their environments, even against a zero-day like one we'll demonstrate.

Join us to learn how attackers search for and exploit vulnerabilities in AWS services to gain access to cloud environments.

- link
- link

SpeakerBio: Nick Frichette, Staff Security Researcher at Datadog

Nick Frichette is a Staff Security Researcher at Datadog, where he specializes in offensive AWS security. He is known for finding multiple zero-day vulnerabilities in AWS services and regularly publishing on new attack techniques. In addition to his research, Nick is the creator and primary contributor to Hacking the Cloud, an open source encyclopedia of offensive security capabilities for cloud environments. He is also a part of the AWS Community Builder Program, where he develops content on AWS security.

Return to Index - Add to Google - ics Calendar file

ADV - Sunday - 11:30-11:59 PDT

Title: Kubernetes Attack Simulation: The Definitive Guide
When: Sunday, Aug 11, 11:30 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

So your organization decided to follow the trend and switched to Kubernetes for hosting their applications. And this means that the mission for the SOC, has now changed from monitoring servers and networks, to building detective capability for a container orchestration platform. Where do you even start with for Kubernetes TTPs? What attack signatures should you alert upon, and what logs are there to look for in first place?

A similar challenge arises for the offensive security practitioner: What strategies exist for performing continuous Kubernetes threat emulation? Infrastructure technologies have changed rapidly, and adversaries have adapted. Despite the novelty of attack surface, insider threats still remain relevant, and prevention alone is not enough to manage the risk posed to the modern enterprise.

This talk will explain the benefits of investing in a proactive approach to the security of your Kubernetes clusters through collaborative purple teams, and will provide a comprehensive guide for doing so – as informed by our latest research and experience in running attack simulations against large enterprises. Attendees will get up to speed with Kubernetes security monitoring concepts and will take away key advice for planning and executing successful attack detection exercises against containerized environments.

SpeakerBio: Leo Tsaousis, Senior Security Consultant at WithSecure

Leo is a Senior Security Consultant at WithSecure where he leads the Attack Path Mapping service. His current role involves planning and conducting collaborative offensive security assessments for large organizations, while building the team globally and pushing the boundaries of threat simulation.

After a brief stint on the defensive side, he returned to consulting with a mission to help SOC teams of all sizes develop their detective capability. To this end, he has been designing and leading purple team exercises for WithSecure’s clients.

His passion for technical research has occasionally led to the discovery of vulnerabilities in products which were assigned CVE IDs and presented at security conferences like ROOTCON and BSides. In his free time, Leo volunteers his skills and experience to help NGOs across the world address their cyber security needs.

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 10:45-12:59 PDT

Title: Kubernetes Security: Hands-On Attack and Defense
When: Sunday, Aug 11, 10:45 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Classroom - Map

Description:

Kubernetes is the de facto operating system of the cloud, more organizations are running their workloads on Kubernetes. While Kubernetes offers many benefits, new users may introduce security risks like cluster misconfiguration, leaked credentials, cryptojacking, container escapes, and vulnerable clusters.

This workshop will teach you the fundamentals of Kubernetes security, from protecting your cluster to securing your workloads. You'll learn about RBAC, OPA, Security Contexts, Network Policies, and other security features. You'll also learn how to exploit workloads running on a Kubernetes environment using Living Off the Land (LotL) techniques like exploiting Insecure APIs, Secrets Theft, Container Escape and Pod Privilege Escalation, similar to the ones used by real-world threat actors.

This workshop is designed for both beginners and advanced students. By the end of the workshop, you'll have a deep understanding of Kubernetes security and the skills to protect your K8S clusters.

SpeakerBio: alevsk

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog https://www.alevsk.com.

Return to Index - Add to Google - ics Calendar file

DDV - Sunday - 10:00-10:59 PDT

Title: Last chance to pick up drives at the DDV
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W225 - Map

Description:

This is your last chance to pickup your drives whether they're finished or not. Get here between 10:00am and 11:00am on Sunday as any drives left behind are considered donations.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 10:00-10:20 PDT

Title: Laundering Money
When: Saturday, Aug 10, 10:00 - 10:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

CSC ServiceWorks is a large vendor of pay-to-play laundry machines in apartments and condomiums. Most are Speed Queens, but newer CSC-branded machines use an app for payment and have custom circuitry inside. Many however accept quarters as well. We show that, when all else fails, you can always physically bypass the coin slot to run the machines for free.

1. link
2. link
3. link
4. link
5. link
6. link
7. link
8. link
9. link
10. link
11. link
12. link
13. link
14. link
15. link
16. link
17. link
18. link
19. link
20. link
21. link

SpeakerBio: Michael Orlitzky

Michael is a programmer, linux developer, network administrator, security consultant, lockpicker, bike messenger, and mathematician from Baltimore. The only thing he hates more than computers is computers inside of other things.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 19:30-21:59 PDT

Title: Lawyers Meet
When: Friday, Aug 9, 19:30 - 21:59 PDT
Where: LVCC West/Floor 2/W228 - Map

Description:

If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join Jeff McNamara for a friendly get-together, drinks, and conversation.

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:15-11:45 PDT

Title: Learn BadUSB Hacking With the USB Nugget
When: Saturday, Aug 10, 10:15 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

In this workshop, you'll learn to write BadUSB scripts to hack computers using a cute, cat-shaped hacking tool called the USB Nugget. You'll learn to write scripts to get computers of any operating system to do your bidding in seconds, and also how to automate nearly any desired action remotely. If you want to learn scripting like the USB Rubber Ducky, but with a Wi-Fi interface and more, this workshop is for you! A computer with Google Chrome is required for this workshop.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 12:00-13:30 PDT

Title: Learn Beginner Soldering With the Meow Mixer Badge
When: Friday, Aug 9, 12:00 - 13:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

In this class, we solder together a light-up, cat-themed badge that teaches a simple RGB tuning circuit. By turning the red, green, or blue knobs, you can adjust the color of the cat's eyes. Perfect for beginners and soldering experts wanting to make a fun and cute badge.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 13:00-14:59 PDT

Title: Learn Zero Trust Network Security with Cloudflare
When: Saturday, Aug 10, 13:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Do you have any photos, videos, games or apps privately hosted at home that you'd love to easily and securely share with your friends anywhere in the world, for free? Would you like to learn how to secure your family and school's Internet access against phishing, ransomware, and other Internet risks? In this hands-on class you will learn how to easily build a secure private network over the Internet with Cloudflare Zero Trust services.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 15:00-16:59 PDT

Title: Learning the New Amass Collection Engine
When: Saturday, Aug 10, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

The OWASP Amass Project has been developing the new OSINT Collection Engine that is designed around the Open Asset Model data standard released last year. The new engine makes your use of Amass more flexible than ever before, yet does come with some additional configurations to learn. This workshop will take users, both new and seasoned, all the way through the experience of using this new architecture.

SpeakerBio: Jeff Foley
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 14:00-14:50 PDT

Title: Level UP OSINT
When: Friday, Aug 9, 14:00 - 14:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

Dive into the dynamic world of Open Source Intelligence (OSINT) with this quick workshop designed to give you a taste of practical online investigations and threat hunting. Led by a seasoned professional, this immersive session offers a condensed yet impactful introduction to essential OSINT techniques that you can use in your red teaming engagements.

Experience the power of hands-on learning as you engage in live demonstrations, exploring key concepts such as operational security (OpSec), advanced search engine queries, username and phone number lookups, social media reconnaissance, breached records analysis, network reconnaissance, historical records, and essential documentation, all within the span of this engaging workshop. Through interactive exercises and guided discussions, participants will gain a glimpse into the world of OSINT.

Who’s it for?

This training is suited for all individuals in any field with a keen interest in online investigations regardless of their experience level in OSINT

SpeakerBio: Mishaal Khan
No BIO available

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 14:30-15:15 PDT

Title: Leveraging AI for Smarter Bug Bounties
When: Saturday, Aug 10, 14:30 - 15:15 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

As security researchers, we constantly attempt to stay ahead of the curve, seeking innovative solutions to enhance our offensive security strategies. In recent years, the advent of artificial intelligence (AI) has introduced a new dimension to our efforts, particularly in the realm of bug bounties and pentesting. While significant attention has been given to understanding and mitigating attacks against AI systems, the potential of AI to assist in the offensive security field remains largely unclear.

This talk pretends to dig into the research and development process undertaken to create an AI agent designed to augment the bug bounty and pentesting workflow. Our AI agent is not merely a theoretical concept but a practical tool aimed at enhancing the efficiency and effectiveness of security researchers.

We have conducted extensive research to understand how AI can mimic and enhance human intuition and creativity in identifying vulnerabilities. While this may sound trivial, there is little evidence of this being tested before on generative AI agents. Our work breaks new ground by pushing the boundaries of what AI can achieve in offensive security.

Will AI become an indispensable tool in our arsenal, capable of autonomously identifying and exploiting vulnerabilities? Join us as we explore the possibilities and implications of AI as an offensive assistant in this new era of offensive security.

Speakers: Diego Jurado,Joel "Niemand_Sec" Noguera

SpeakerBio: Diego Jurado, Security Researcher at XBOW

Diego Jurado is a security researcher at XBOW, a company dedicated to developing innovative AI for offensive security. Diego is an offensive security professional with an extensive background in bug bounty, penetration testing and red team. Prior to this role, Diego has held positions at companies such as Microsoft Xbox, Activision Blizzard King and Telefónica. Additionally, Diego participates in bug bounty programs and has managed to establish himself in the top 38 all time leaderboard of HackerOne. Diego is part of Team Spain, champion of the Ambassadors World Cup 2023 a bug bounty competition organized by HackerOne.

SpeakerBio: Joel "Niemand_Sec" Noguera, Security Researcher at XBOW

Joel Noguera is a security researcher at XBOW, a company dedicated to developing innovative AI for offensive security. Joel is a security professional and bug hunter with more than eight years of expertise in exploit development, reverse engineering, security research and consulting. He has actively participated in Bug Bounty programs since 2016, reaching the all-time top 60 on the HackerOne leaderboard. Before joining XBOW, he was part of Immunity Inc., where he worked as a security researcher for three years. Joel has presented at Recon, BlackHat Europe, EkoParty and BSides Keynote Berlin, among others.

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 10:00-10:59 PDT

Title: Leveraging Internal Systems for Enhanced Bug Bounty Success
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

Every bug hunter knows the initial steps: reconnaissance, fuzzing, and asset enumeration, But what if I told you there's a way to get everything you need internally and have it handed to you on a silver platter? Join me as I share my journey as part of different security teams across my career. I'll reveal the methods and tricks I've developed to utilize internal systems to retrieve crucial data, significantly boosting productivity in finding and exploiting flaws in our code. I'll present success stories and real-life examples where researchers uncovered critical vulnerabilities with internal assistance. Additionally, I'll delve into the tactics and techniques I employ to obtain this valuable data, providing program owners with insights to elevate their game—if they dare to expose this information.

SpeakerBio: Rotem Bar

Rotem Bar is a dedicated cybersecurity expert with over ten years of experience, focusing on internal security using bug bounty programs and other pentesting capabilities. His passion for identifying and mitigating security vulnerabilities has led him to actively participate in numerous security initiatives, earning recognition within the community.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 16:30-17:15 PDT

Title: Leveraging private APNs for mobile network traffic analysis
When: Friday, Aug 9, 16:30 - 17:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Knowing where and how your mobile and IoT devices communicate on the Internet is essential for ensuring privacy and security.

In the past, it has been easy to follow their communication through a WIFI connection that you control. However, your devices are becoming more locked down and utilize mobile networks such as 4G and 5G for communication. As the devices communicate directly through mobile network base stations operated by Internet Service Providers (ISPs), tampering with or even monitoring their communication is outside your reach.

While it is possible to set up a private base station, it requires expensive components and is hard to operate. However, many ISPs have begun offering private Access Point Names (APNs) to allow you to have a private network inside the ISP infrastructure.

This talk will show how you can affordably leverage ISP-operated mobile networks and their private APN services to control your mobile devices' network traffic. This technique lets you inspect, filter, and tamper with your mobile devices' IP traffic for offensive and defensive cyber security needs, such as penetration testing IoT devices or monitoring mobile device endpoints for malicious traffic.

- link
- Janne Taponen - Economizing Mobile Network Warfare: Budget-Friendly Baseband Fuzzing - T2 2024 Conference
- XiaoHuiHui - All the 4G Modules Could Be Hacked - DEF CON 27 Conference link

SpeakerBio: Aapo Oksman, Founder at Juurin Oy

Aapo Oksman is an entrepreneur and the Founder of Juurin Oy, a boutique company focusing on technical IoT cybersecurity. His background is in electrical engineering, embedded devices, and test automation. Combining his background with a hacking hobby led to a cybersecurity career focusing on industrial IoT.

Bug Bounties and security research keep Aapo motivated and learning. His work in PKI and TLS has resulted in multiple CVEs from vendors like Microsoft, Google, Apple, and Samsung. At DEF CON 31, Aapo released a TLS hacking tool, certmitm, that has proven its worth in finding insecure TLS implementations with new vulnerabilities found constantly.

Outside work and research, Aapo's passion is in the community. He organizes local security meetups and coaches the Finnish national youth CTF team in the yearly European Cybersecurity Challenge competition.

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 16:30-17:59 PDT

Title: LFG! Forming a Bug Bounty Hunting Party
When: Friday, Aug 9, 16:30 - 17:59 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

James "Jimmy" Donaldson, better known by his online handle Mr. Beast, is the most successful YouTuber of all time. The digital superstar has often spoken about how learning to make digital content with a group was the reason he was able to grow so quickly. By collaborating with a small cohort of people who shared his passion, each individual was able to not only learn from one another's unique skills, but most importantly, they learned from each other's failures and made corrections to avoid those pitfalls themselves. This workshop is designed to help you learn to apply this same principle to Bug Bounty Hunting and grow exponentially faster than you can on your own.

After sharing some success stories from his own journey, Harrison Richardson (rs0n) will lead the audience in forming small bug bounty hunting groups optimized for success. Attendees will be grouped based on their technical skills, bug bounty experience, and work experience to build an effective cohort. Next, rs0n will guide each group in selecting a public Bug Bounty Program based on their combined skills and will coach the groups individually on working together to find and report bugs. Special emphasis will be placed on learning to take essential notes and build a custom hunting methodology that works for you and your team. Finally, rs0n will host a live Q&A session to answer any "burning" questions the participants have about bug bounty hunting and/or transitioning to a career of Application Security.

There have been massive strides made in the bug bounty industry over the past few years, but one problem continues to persist. Researchers at all levels view other bug bounty hunters as competition who will steal their techniques. The goal of this workshop is not only to teach the skills needed to effectively collaborate on bug bounty programs, but also to demonstrate the immense value of collaboration when learning offensive security.

SpeakerBio: Harrison Richardson

Harrison Richardson (rs0n) began his Cybersecurity career in the US Army as a 25B. After leaving the service, Harrison worked various contract and freelance jobs while completing his Masters in Cybersecurity from the University of Dallas. Harrison's first full-time job in the civilian sector was at Rapid7, where he worked as a senior security solutions engineer as part of their Applied Engineering Team. Today, Harrison is the security engineering manager for the FloQast Security Team, specifically overseeing application security. In his free time, Harrison works to provide educational content to the bug bounty community through YouTube and Twitch.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: LHC Meshtastic Activities and CTF
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Lonely Hackers Club is conducting some meshtastic activities during DEF CON 32.

The Lonely Hackers Club is hosting a CTF over Meshtastic. To participate you will need a Meshtastic node. There will be additional flags located in or near the LHC room. For more information check out our Meshtastic page.

Getting Started

Learn more here.

Default LongFast Mesh + LHC Channel, Use before DEF CON

Tap here to reconfigure your device

DEFCONnect ShortFast Mesh + LHC Channel, Use during DEF CON

Tap here to reconfigure your device

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: LHC Meshtastic Activities and CTF
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Lonely Hackers Club is conducting some meshtastic activities during DEF CON 32.

The Lonely Hackers Club is hosting a CTF over Meshtastic. To participate you will need a Meshtastic node. There will be additional flags located in or near the LHC room. For more information check out our Meshtastic page.

Getting Started

Learn more here.

Default LongFast Mesh + LHC Channel, Use before DEF CON

Tap here to reconfigure your device

DEFCONnect ShortFast Mesh + LHC Channel, Use during DEF CON

Tap here to reconfigure your device

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: LHC Meshtastic Activities and CTF
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Lonely Hackers Club is conducting some meshtastic activities during DEF CON 32.

The Lonely Hackers Club is hosting a CTF over Meshtastic. To participate you will need a Meshtastic node. There will be additional flags located in or near the LHC room. For more information check out our Meshtastic page.

Getting Started

Learn more here.

Default LongFast Mesh + LHC Channel, Use before DEF CON

Tap here to reconfigure your device

DEFCONnect ShortFast Mesh + LHC Channel, Use during DEF CON

Tap here to reconfigure your device

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: LHC's Unofficial Sticker Swap Table
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

The Unofficial Sticker Swap is a casual and engaging activity where attendees can trade and collect unique stickers. This event fosters a sense of community and allows participants to showcase their creativity and personal style.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-11:59 PDT

Title: LHC's Unofficial Sticker Swap Table
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

The Unofficial Sticker Swap is a casual and engaging activity where attendees can trade and collect unique stickers. This event fosters a sense of community and allows participants to showcase their creativity and personal style.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: LHC's Unofficial Sticker Swap Table
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

The Unofficial Sticker Swap is a casual and engaging activity where attendees can trade and collect unique stickers. This event fosters a sense of community and allows participants to showcase their creativity and personal style.

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 15:00-15:59 PDT

Title: Life, Liberty and the pursuit of Convenience: the slow death of independence
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Over the years, while people have expressed more and more concern about what freedoms we have in the US, less and less understanding of what true freedom means has been demonstrated. Here, we take a look at the related definitions, and how technology has been both a secret advocate and opponent of the freedoms we claim to desire so much.

SpeakerBio: Kaleeque Pierce, Management Professional
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Wednesday - 17:00-05:59 PDT

Title: Linecon
When: Wednesday, Aug 7, 17:00 - 05:59 PDT
Where: LVCC West - Map

Description:

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Please also review the "Human Registration Open" event, and familiarize yourself with the **important notes** therein.

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Linux Trainer
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Knowing how to use the Linux command line is a critical skill for any good security practitioner. This trainer will have 10+ problems covering some of the most fundamental Linux commands. This trainer is for people new to field and for those who want to hone their Linux command line-fu.

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Linux Trainer
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Knowing how to use the Linux command line is a critical skill for any good security practitioner. This trainer will have 10+ problems covering some of the most fundamental Linux commands. This trainer is for people new to field and for those who want to hone their Linux command line-fu.

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Linux Trainer
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Knowing how to use the Linux command line is a critical skill for any good security practitioner. This trainer will have 10+ problems covering some of the most fundamental Linux commands. This trainer is for people new to field and for those who want to hone their Linux command line-fu.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 11:30-12:15 PDT

Title: Listen to the whispers: web timing attacks that actually work
When: Friday, Aug 9, 11:30 - 12:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Websites are riddled with timing oracles eager to divulge their innermost secrets. It's time we started listening to them.

In this session, I'll unleash novel attack concepts to coax out server secrets including masked misconfigurations, blind data-structure injection, hidden routes to forbidden areas, and a vast expanse of invisible attack-surface.

This is not a theoretical threat; every technique will be illustrated with multiple real-world case studies on diverse targets. Unprecedented advances have made these attacks both accurate and efficient; in the space of ten seconds you can now reliably detect a sub-millisecond differential with no prior configuration or 'lab conditions' required. In other words, I'm going to share timing attacks you can actually use.

To help, I'll equip you with a suite of battle-tested open-source tools enabling both hands-free automated exploitation, and custom attack scripting. I'll also share a little CTF to help you hone your new skillset.

Want to take things further? I'll help you transform your own attack ideas from theory to reality, by sharing a methodology refined through testing countless concepts on thousands of websites. We've neglected this omnipresent and incredibly powerful side-channel for too long.

- link
- link

SpeakerBio: James "albinowax" Kettle, Director of Research at PortSwigger

James 'albinowax' Kettle is the Director of Research at PortSwigger, the makers of Burp Suite. He's best known for his HTTP Desync Attacks research, which popularised HTTP Request Smuggling. James has extensive experience cultivating novel attack techniques, including web cache poisoning, browser-powered desync attacks, server-side template injection, and password reset poisoning. James is also the author of multiple popular open-source tools including Param Miner, Turbo Intruder, and HTTP Request Smuggler. He is a frequent speaker at numerous prestigious venues including both Black Hat USA and EU, OWASP AppSec USA and EU, and DEF CON.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Live Recon Contest in Progress
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Do you fancy doing live recon on Real Organizations? Then activate Yourself. And compete in a unique HACKER challenge.

This year we are launching a new nail biting Contest, i.e Live Recon where participants will compete with each other to perform a deep osint and recon on the target organization. Here are the details:

About the contest:

Join us for an electrifying two-day Live Reconnaissance Event. Whether you're a seasoned security expert, a curious newcomer or a bugbounty pro, this is your chance to test your skills in a high-octane environment.

Your Mission

Get ready to perform live reconnaissance on a curated list of companies. Dig deep and unearth critical information that could be game-changing. Use your analytical prowess and sharp instincts to explore, probe, and uncover hidden data.

Why Join the Hunt?

Experience Real-World Challenges: Face off against real-world scenarios. Compete and Collaborate: Work with the best minds in the field. Learn from the Masters: Recon on a massive scale. Score Epic Prizes: Walk away with cool rewards.

Who's Invited?

If you've got a passion for cybersecurity and Recon, this event is for you. Whether you're a university student, a pro pentester, or a hobbyist eager to sharpen your skills, we want you! Teams are encouraged to register and bring a mix of talents to tackle these challenges head-on.

Get Ready to Recon!

Unleash your inner hacker and join us for a reconnaissance adventure you won't forget!

Please note that this is an in-person event, and winners need to be at DEFCON to collect their prizes. However, once we have announced the targets, participants can play it from anywhere online (as this is Recon on public and live targets).

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-12:59 PDT

Title: Live Recon Contest in Progress
When: Saturday, Aug 10, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Do you fancy doing live recon on Real Organizations? Then activate Yourself. And compete in a unique HACKER challenge.

This year we are launching a new nail biting Contest, i.e Live Recon where participants will compete with each other to perform a deep osint and recon on the target organization. Here are the details:

About the contest:

Join us for an electrifying two-day Live Reconnaissance Event. Whether you're a seasoned security expert, a curious newcomer or a bugbounty pro, this is your chance to test your skills in a high-octane environment.

Your Mission

Get ready to perform live reconnaissance on a curated list of companies. Dig deep and unearth critical information that could be game-changing. Use your analytical prowess and sharp instincts to explore, probe, and uncover hidden data.

Why Join the Hunt?

Experience Real-World Challenges: Face off against real-world scenarios. Compete and Collaborate: Work with the best minds in the field. Learn from the Masters: Recon on a massive scale. Score Epic Prizes: Walk away with cool rewards.

Who's Invited?

If you've got a passion for cybersecurity and Recon, this event is for you. Whether you're a university student, a pro pentester, or a hobbyist eager to sharpen your skills, we want you! Teams are encouraged to register and bring a mix of talents to tackle these challenges head-on.

Get Ready to Recon!

Unleash your inner hacker and join us for a reconnaissance adventure you won't forget!

Please note that this is an in-person event, and winners need to be at DEFCON to collect their prizes. However, once we have announced the targets, participants can play it from anywhere online (as this is Recon on public and live targets).

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 16:00-17:59 PDT

Title: Live Recon Finalist Presentations
When: Saturday, Aug 10, 16:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 13:00-15:59 PDT

Title: Live Recon Finalist Selection Process
When: Saturday, Aug 10, 13:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Join Drew Green, John Rodriguez, and Ken Pyle for a deep dive into identifying vulnerabilities in network devices. Explore and exploit weaknesses in a wireless mesh network and learn how advanced threats view your infrastructure.

Speakers: Drew Green,John Rodriguez,Ken Pyle

SpeakerBio: Drew Green
No BIO available
SpeakerBio: John Rodriguez
No BIO available
SpeakerBio: Ken Pyle
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Join Drew Green, John Rodriguez, and Ken Pyle for a deep dive into identifying vulnerabilities in network devices. Explore and exploit weaknesses in a wireless mesh network and learn how advanced threats view your infrastructure.

Speakers: Drew Green,John Rodriguez,Ken Pyle

SpeakerBio: Drew Green
No BIO available
SpeakerBio: John Rodriguez
No BIO available
SpeakerBio: Ken Pyle
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Join Drew Green, John Rodriguez, and Ken Pyle for a deep dive into identifying vulnerabilities in network devices. Explore and exploit weaknesses in a wireless mesh network and learn how advanced threats view your infrastructure.

Speakers: Drew Green,John Rodriguez,Ken Pyle

SpeakerBio: Drew Green
No BIO available
SpeakerBio: John Rodriguez
No BIO available
SpeakerBio: Ken Pyle
No BIO available

Return to Index - Add to Google - ics Calendar file

LPV - Friday - 10:00-17:59 PDT

Title: Lockpicking Activities
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03-A - Map

Description:

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

A popular spot for new lock pickers! Highly recommended you stop by. The Lockpick Village is always kid friendly and welcomes folks of all ages. We do require that the parents stay with the kids.

Return to Index - Add to Google - ics Calendar file

LPV - Sunday - 10:00-12:59 PDT

Title: Lockpicking Activities
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03-A - Map

Description:

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

A popular spot for new lock pickers! Highly recommended you stop by. The Lockpick Village is always kid friendly and welcomes folks of all ages. We do require that the parents stay with the kids.

Return to Index - Add to Google - ics Calendar file

LPV - Saturday - 10:00-17:59 PDT

Title: Lockpicking Activities
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03-A - Map

Description:

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

A popular spot for new lock pickers! Highly recommended you stop by. The Lockpick Village is always kid friendly and welcomes folks of all ages. We do require that the parents stay with the kids.

Return to Index - Add to Google - ics Calendar file

LPV - Saturday - 13:00-13:30 PDT

Title: Locksport Competitions: Compete in the Olympics of Locks
When: Saturday, Aug 10, 13:00 - 13:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Picking locks is fun, but what if you want more? Ever considered competing against other lock enthusiasts? In this talk we'll discuss the exciting lock-related competitions that take place around the world, how to find them, and what it takes to compete and win.

SpeakerBio: Matt Burrough

Matt Burrough is a devoted locksport hobbyist who has competed in a variety of international lockpicking tournaments. He also co-leads the Seattle Locksport group. During the day, Matt manages a professional red team. He is the author of Pentesting Azure Applications (No Starch Press, 2018) and co-author of Locksport (No Starch Press, 2024).

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Lonely Hackers Club Community Room Open
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Lonely Hackers Club Community Room Open
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Lonely Hackers Club Community Room Open
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Lonely Hard Drive
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

You have been randomly selected for additional security training. Be on the look out for one of our drives, USBs or surprise devices out here in Vegas, and follow along on @LonelyHardDrive for further clues to start hacking away at the puzzles. This is required for all LonelyCorp employees and Betty Pagefile is counting on you!

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Lonely Hard Drive
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

You have been randomly selected for additional security training. Be on the look out for one of our drives, USBs or surprise devices out here in Vegas, and follow along on @LonelyHardDrive for further clues to start hacking away at the puzzles. This is required for all LonelyCorp employees and Betty Pagefile is counting on you!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Lonely Hard Drive
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

You have been randomly selected for additional security training. Be on the look out for one of our drives, USBs or surprise devices out here in Vegas, and follow along on @LonelyHardDrive for further clues to start hacking away at the puzzles. This is required for all LonelyCorp employees and Betty Pagefile is counting on you!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Lonely Tag
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

How far will you go? Or, more accurately, how far was your tag's last reported location? Pre-register your team to receive one of a dozen tags, and check out our socials (@LonelyHardDrive) to watch the tags move across the map!

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Lonely Tag
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

How far will you go? Or, more accurately, how far was your tag's last reported location? Pre-register your team to receive one of a dozen tags, and check out our socials (@LonelyHardDrive) to watch the tags move across the map!

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Lonely Tag
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-F - Map

Description:

How far will you go? Or, more accurately, how far was your tag's last reported location? Pre-register your team to receive one of a dozen tags, and check out our socials (@LonelyHardDrive) to watch the tags move across the map!

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 12:00-13:59 PDT

Title: LoRa for Hackers : Long Range Hacking for Beginners With CircuitPython
When: Saturday, Aug 10, 12:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

LoRa is an exciting new technology renowned for its low cost and long range, making it popular for hackers and makers. In this workshop, you'll learn to program a LoRa radio with CircuitPython to create long-range hacking tools and blinky prototypes which can communicate off-grid from over a mile away! The workshop will cover remotely triggered BadUSB devices, LED controllers, sensor monitors, and more! A computer with Google Chrome is required for this workshop.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 08:00-01:59 PDT

Title: Lost & Found
When: Friday, Aug 9, 08:00 - 01:59 PDT
Where: LVCC West/Floor 2/W238 - Map

Description:

If you find something that seems to have been lost, please take that item to the nearest NFO Node. The item will enter the DEF CON Lost & Found system.

If you've lost something, the only way to check on it (or reclaim it) is by going to the Lost & Found department yourself. The Lost & Found department is in room LVCC - L2 - W238. You may also call Lost & Found at +1 (725) 377-5045.

The Lost & Found department plans to be open Thursday - Saturday, during all hours that the conference operates. On Sunday, the Lost & Found department will open with the venue at 08:00, but will close at the beginning of DEF CON 32 Closing Ceremonies (15:00). Shortly thereafter, all remaining lost items will be transferred to the LVCC West Lobby Security Office. If you need to reach LVCC's West Lobby Security Office, you may call +1 (702) 943-3532.

Return to Index - Add to Google - ics Calendar file

MISC - Thursday - 07:00-01:59 PDT

Title: Lost & Found
When: Thursday, Aug 8, 07:00 - 01:59 PDT
Where: LVCC West/Floor 2/W238 - Map

Description:

If you find something that seems to have been lost, please take that item to the nearest NFO Node. The item will enter the DEF CON Lost & Found system.

If you've lost something, the only way to check on it (or reclaim it) is by going to the Lost & Found department yourself. The Lost & Found department is in room LVCC - L2 - W238. You may also call Lost & Found at +1 (725) 377-5045.

The Lost & Found department plans to be open Thursday - Saturday, during all hours that the conference operates. On Sunday, the Lost & Found department will open with the venue at 08:00, but will close at the beginning of DEF CON 32 Closing Ceremonies (15:00). Shortly thereafter, all remaining lost items will be transferred to the LVCC West Lobby Security Office. If you need to reach LVCC's West Lobby Security Office, you may call +1 (702) 943-3532.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 08:00-14:59 PDT

Title: Lost & Found
When: Sunday, Aug 11, 08:00 - 14:59 PDT
Where: LVCC West/Floor 2/W238 - Map

Description:

If you find something that seems to have been lost, please take that item to the nearest NFO Node. The item will enter the DEF CON Lost & Found system.

If you've lost something, the only way to check on it (or reclaim it) is by going to the Lost & Found department yourself. The Lost & Found department is in room LVCC - L2 - W238. You may also call Lost & Found at +1 (725) 377-5045.

The Lost & Found department plans to be open Thursday - Saturday, during all hours that the conference operates. On Sunday, the Lost & Found department will open with the venue at 08:00, but will close at the beginning of DEF CON 32 Closing Ceremonies (15:00). Shortly thereafter, all remaining lost items will be transferred to the LVCC West Lobby Security Office. If you need to reach LVCC's West Lobby Security Office, you may call +1 (702) 943-3532.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 08:00-01:59 PDT

Title: Lost & Found
When: Saturday, Aug 10, 08:00 - 01:59 PDT
Where: LVCC West/Floor 2/W238 - Map

Description:

If you find something that seems to have been lost, please take that item to the nearest NFO Node. The item will enter the DEF CON Lost & Found system.

If you've lost something, the only way to check on it (or reclaim it) is by going to the Lost & Found department yourself. The Lost & Found department is in room LVCC - L2 - W238. You may also call Lost & Found at +1 (725) 377-5045.

The Lost & Found department plans to be open Thursday - Saturday, during all hours that the conference operates. On Sunday, the Lost & Found department will open with the venue at 08:00, but will close at the beginning of DEF CON 32 Closing Ceremonies (15:00). Shortly thereafter, all remaining lost items will be transferred to the LVCC West Lobby Security Office. If you need to reach LVCC's West Lobby Security Office, you may call +1 (702) 943-3532.

Return to Index - Add to Google - ics Calendar file

BBV - Sunday - 11:00-12:30 PDT

Title: Lost in Translation - WAF Bypasses By Abusing Data Manipulation Processes
When: Sunday, Aug 11, 11:00 - 12:30 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

In today's dynamic web application ecosystem, there exists numerous data manipulation processes to sanitize, translate and manipulate data for use by applications, for storage in back-end systems or sent to clients in web browsers. These same processes, however, can also be leveraged by bug hunters to obfuscate attack payloads from intermediary security systems such as web application firewalls (WAFs). In this workshop we will discuss several abuse scenarios including Edge-Side Includes (ESI), XSS Sanitizers and Unicode Normalizations.

Pre-Requisites: Hands-on labs will be hosted on YesWeHack's free DOJO platform (https://dojo-yeswehack.com/). Participants are encouraged to sign up for an account in advance and will use their own laptops for labs.

Speakers:
Ryan Barnett,Isabella Barnett

SpeakerBio:
Ryan Barnett, Akamai

Ryan Barnett is a Principal Security Researcher working on the Akamai Threat Research Team supporting the App and API Protector product. In addition to his primary work at Akamai, he is also a former Faculty Member for the SANS Institute, a WASC Board Member and OWASP Project Leader for: ModSecurity Core Rule Set (CRS) Web Hacking Incident Database (WHID). Mr. Barnett has also authored two web security books: Preventing Web Attacks with Apache (Pearson) and The Web Application Defender's Cookbook: Battling Hackers and Defending Users (Wiley).

SpeakerBio:
Isabella Barnett

Isabella Barnett is a Software Engineering Intern at Databuoy and a rising freshman at George Mason Honor's College studying Cyber Security Engineering.

Return to Index - Add to Google - ics Calendar file

HRV - Saturday - 14:00-14:30 PDT

Title: Low Power & Long Range Communications - QRP
When: Saturday, Aug 10, 14:00 - 14:30 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

In this talk we'll cover just how far you can communicate on less power than your phone uses to charge. How to tx over the horizon and how to power it all.

SpeakerBio: Escobar

Eric is a seasoned penetration tester by day an amateur extra by night (W6WD).

Return to Index - Add to Google - ics Calendar file

Title: Mac-n-Cheese: How to Cook Up Delicious Electron Techniques for Red Teamers
When: Friday, Aug 9, 16:00 - 16:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

In the world of cybersecurity, the kitchen is always hot, and at this year's Defcon in Las Vegas, we're cooking up something special in the Red Team Village. Our dish of the day? A deep dive into the exploitation of Electron applications, served with a side of humor and a dash of intrigue.

Electron applications, while popular, have been found to have a soft underbelly. This talk will demonstrate how these applications can be abused to access directories protected by the Transparency, Consent, and Control (TCC) framework. We'll also show how these applications can be manipulated to maintain persistence by inserting backdoors, effectively turning them into bridges for privilege escalation.

We'll walk you through the anatomy of an Electron app, laying out the exploitation scenarios in detail. We'll serve up a course of case studies, featuring apps that were once vulnerable but have since been patched, and those that remain vulnerable because their manufacturers do not consider these issues as vulnerabilities (let's see if after this talk they won't fix it). These examples will highlight the loopholes that both red team simulations and real attackers can exploit.

Our menu will also include a discussion on the importance of hardening Electron applications. Without proper hardening, these apps can easily be used as access points for privilege escalation and backdoor implantation. We'll present techniques that cater to the unique characteristics of some apps, which have diverse permissions in the system.

For dessert, we'll delve into the more sinister side of these vulnerabilities. Some applications have entitlements that enable access to the camera and audio, which can be exploited to monitor victims. We'll demonstrate how these entitlements can be abused, adding a chilling finish to our meal.

Throughout the talk, we'll be showcasing XX CVE's that we've acquired, providing a real-world context to our discussion. We'll also demonstrate two tools that we've created, which will add some spice to our presentation.

So, join us as we whip up a batch of Mac-n-Cheese, serving you delicious Electron techniques that will leave you hungry for more. This talk is a must-attend for anyone interested in understanding the potential vulnerabilities in Electron applications and how to exploit them. Bon appétit, Red Teamers!

SpeakerBio: Roberto Soares
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 13:00-13:50 PDT

Title: macOS Red Team on Corporate Scenarios
When: Saturday, Aug 10, 13:00 - 13:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

In this research businesses and organizations continue to adopt more advanced security measures to protect against cyber-attacks on your macOS endpoints, attackers are constantly evolving their techniques to bypass these measures. In this presentation, we will demonstrate real-world attack scenarios and reveal common vulnerabilities, as well as provide insights on how to exploit them. "macOS Red Team on Corporate Scenarios" is the result of years of research and dedicated work in testing macOS environments. Its main objective is to provide a comprehensive view of the security surrounding Apple's operating system, demonstrating how potential vulnerabilities can be exploited. The adopted approach assumes the perspective of an insider attacker or during a Red Team simulation.

The research will delve into various security features embedded within macOS, such as SIP (System Integrity Protection), TCC (Transparency, Consent, and Control), FileVault, SSV (System Software Version), Gatekeeper, XProtect, and Secure Boot. These components play crucial roles in safeguarding the integrity, privacy, and overall security posture of the macOS operating system.

The research will also delve into the tactics, techniques, and procedures (TTPs) recommended by the MITRE ATT&CK framework for macOS systems to assist in conducting red team simulations. This exploration aims to provide insights into the methodologies and strategies employed by attackers, enhancing the effectiveness of defensive strategies and improving overall cybersecurity posture in macOS environments.

At the conclusion of the presentation, we will demonstrate how to perform a bypass of a vulnerability discovered in the macOS Transparency, Consent, and Control (TCC) framework. This vulnerability has been reported to Apple for investigation and mitigation. We will also discuss the process of how Apple has handled the vulnerability disclosure and the steps taken by the company to address the issue.

SpeakerBio: Ricardo L0gan
No BIO available

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 10:00-11:45 PDT

Title: Maestro
When: Saturday, Aug 10, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W303 - Map

Description:

Maestro is a post-exploitation tool designed to interact with Intune/EntraID from a C2 agent on a user's workstation without requiring knowledge of the user's password or Azure authentication flows, token manipulation, and web-based administration console. Maestro makes interacting with Intune and EntraID from C2 much easier, as the operator does not need to obtain the user's cleartext password, extract primary refresh token (PRT) cookies from the system, run additional tools or a browser session over a SOCKS proxy, or deal with Azure authentication flows, tokens, or conditional access policies in order to execute actions in Azure on behalf of the logged-in user. Maestro enables attack paths between on-prem and Azure. For example, by running Maestro on an Intune admin's machine, you can execute PowerShell scripts on any enrolled device without ever knowing the admin's credentials!

SpeakerBio: Chris Thompson, Principal Consultant at SpecterOps

Chris Thompson (@_Mayyhem) is a Principal Consultant at SpecterOps, where he conducts red team operations, research, tool development, and training. Chris has instructed at Black Hat USA/EU and spoken at Arsenal, DEF CON Demo Labs, SO-CON, and Troopers. He is the primary author of Maestro and SharpSCCM and co-author of Misconfiguration Manager, an open-source tool and knowledge base that can be used to help demonstrate, mitigate, and detect attacks that abuse Microsoft Configuration Manager (formerly SCCM).

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 14:30-14:59 PDT

Title: Make all the things - Construa seus próprios "brinquedos" Threats
When: Saturday, Aug 10, 14:30 - 14:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Embora tragam muita diversão e inovação, brinquedos conectados à Internet (IoToys) também apresentam sérios riscos à segurança e privacidade. Ao entender e mitigar esses riscos, e até mesmo criando seus próprios dispositivos, pais e responsáveis podem garantir que a diversão com brinquedos inteligentes e conectados não se transforme em uma preocupação com vazamentos de informações pessoais.

SpeakerBio: Christiane Borges Santos, Coordenadora do Eixo de Design Factory - Criar IFG

Tecnóloga em Redes de Comunicação e Mestre em Engenharia Elétrica e da Computação. Fundadora do Grupo de Robótica para Meninas Metabotix e membro do Grupo de Robótica GYNBOT. Atualmente, professora no Instituto Federal de Goiás (IFG) campus Luziânia, Instrutora CISCO NetAcad e Coordenadora do Eixo de Design Factory do Criar Polo de Inovação do IFG.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 16:00-16:59 PDT

Title: Making the DEF CON 32 Badge
When: Friday, Aug 9, 16:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:
SpeakerBio: Mar Williams
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Saturday - 10:00-11:59 PDT

Title: Maltego Community Workshop
When: Saturday, Aug 10, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This workshop aims to describe how to use Maltego CE with the common available transform sets. Additionally we will teach you how to extend the tool by integrating external datasources and OSINT tools thanks to the open-source maltego-trx library.

Outline: - Overview - Datasources - Investigation basics - Creating your own entities - Building your own transforms - Demo - Lab: - Connecting an OSINT tool (holehe, whatsmyname…)
- Q&A

Prerequisites - Maltego Community Edition (requires Maltego ID registration for activation) - Python + pip - Maltego-trx library - Optional: your favourite IDE (VSCode, Pycharm…)

SpeakerBio: Carlos Fragoso
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Malware Contests: MARC I & BOMBE
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-03 - Map

Description:

MARC I: Malware Analysis Report Competition I

In MARC I (Malware Analysis Report Competition I), participants collect and analyze real malware, then write an analysis report like a story, covering the entire scope of who, what, when, where, why, and how they found and analyzed the malware.

MARC I was created by Lena Yu (aka LambdaMamba) to provide malware enthusiasts with an opportunity to learn and showcase their passion and skills. Mastering malware analysis means mastering language. Essentially, we take a highly technical concept and simplify it into something that many can understand, similar to how a compiler translates high-level language into low-level language that a wide range of systems can understand.

When participants open-source and publish their work, it greatly contributes to improving the field of cyber defense. Let's make malware analysis knowledge go viral!

BOMBE: Battle of Malware Bypass and EDR

Try to capture malware by writing your own EDR, or become the malware to bypass detection! BOMBE (Battle of Malware Bypass and EDR) is a unique match where malware and EDR systems compete against each other inside a single VM boxing ring.

Our participants can choose if they want to be malware creator or EDR developer. Malware creators aim to exfiltrate credentials and transmit them to our designated server. On the other side, EDR developers will focus on detecting the malware's activities and report its findings. Both the malware and EDR, created by our participants, will battle each other directly inside a single VM. As they face off, they'll earn points for wins, moving up on the leaderboard. We also encourage them to keep improving their malware or EDR systems, system logs will be released after a few rounds.

BOMBE was created by Wei-Chieh Chao (aka oalieno) and Tien-Chih Lin (aka Dange). It is not just a competition, it's a learning platform. Participants engage with real-world scenarios, learning the circumstances between malware and EDR, a never-ending bypass and detect game. Showcase your skills! Whether you're a wizard at weaving undetectable malware or a mastermind in sophisticated defenses, this is your stage. Demonstrate your capabilities to a global audience, including potential employers and industry leaders.

Return to Index - Add to Google - ics Calendar file

Title: Malware Contests: MARC I & BOMBE
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-03 - Map

Description:

MARC I: Malware Analysis Report Competition I

In MARC I (Malware Analysis Report Competition I), participants collect and analyze real malware, then write an analysis report like a story, covering the entire scope of who, what, when, where, why, and how they found and analyzed the malware.

MARC I was created by Lena Yu (aka LambdaMamba) to provide malware enthusiasts with an opportunity to learn and showcase their passion and skills. Mastering malware analysis means mastering language. Essentially, we take a highly technical concept and simplify it into something that many can understand, similar to how a compiler translates high-level language into low-level language that a wide range of systems can understand.

When participants open-source and publish their work, it greatly contributes to improving the field of cyber defense. Let's make malware analysis knowledge go viral!

BOMBE: Battle of Malware Bypass and EDR

Try to capture malware by writing your own EDR, or become the malware to bypass detection! BOMBE (Battle of Malware Bypass and EDR) is a unique match where malware and EDR systems compete against each other inside a single VM boxing ring.

Our participants can choose if they want to be malware creator or EDR developer. Malware creators aim to exfiltrate credentials and transmit them to our designated server. On the other side, EDR developers will focus on detecting the malware's activities and report its findings. Both the malware and EDR, created by our participants, will battle each other directly inside a single VM. As they face off, they'll earn points for wins, moving up on the leaderboard. We also encourage them to keep improving their malware or EDR systems, system logs will be released after a few rounds.

BOMBE was created by Wei-Chieh Chao (aka oalieno) and Tien-Chih Lin (aka Dange). It is not just a competition, it's a learning platform. Participants engage with real-world scenarios, learning the circumstances between malware and EDR, a never-ending bypass and detect game. Showcase your skills! Whether you're a wizard at weaving undetectable malware or a mastermind in sophisticated defenses, this is your stage. Demonstrate your capabilities to a global audience, including potential employers and industry leaders.

Return to Index - Add to Google - ics Calendar file

Title: Malware Contests: MARC I & BOMBE
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-03 - Map

Description:

MARC I: Malware Analysis Report Competition I

In MARC I (Malware Analysis Report Competition I), participants collect and analyze real malware, then write an analysis report like a story, covering the entire scope of who, what, when, where, why, and how they found and analyzed the malware.

MARC I was created by Lena Yu (aka LambdaMamba) to provide malware enthusiasts with an opportunity to learn and showcase their passion and skills. Mastering malware analysis means mastering language. Essentially, we take a highly technical concept and simplify it into something that many can understand, similar to how a compiler translates high-level language into low-level language that a wide range of systems can understand.

When participants open-source and publish their work, it greatly contributes to improving the field of cyber defense. Let's make malware analysis knowledge go viral!

BOMBE: Battle of Malware Bypass and EDR

Try to capture malware by writing your own EDR, or become the malware to bypass detection! BOMBE (Battle of Malware Bypass and EDR) is a unique match where malware and EDR systems compete against each other inside a single VM boxing ring.

Our participants can choose if they want to be malware creator or EDR developer. Malware creators aim to exfiltrate credentials and transmit them to our designated server. On the other side, EDR developers will focus on detecting the malware's activities and report its findings. Both the malware and EDR, created by our participants, will battle each other directly inside a single VM. As they face off, they'll earn points for wins, moving up on the leaderboard. We also encourage them to keep improving their malware or EDR systems, system logs will be released after a few rounds.

BOMBE was created by Wei-Chieh Chao (aka oalieno) and Tien-Chih Lin (aka Dange). It is not just a competition, it's a learning platform. Participants engage with real-world scenarios, learning the circumstances between malware and EDR, a never-ending bypass and detect game. Showcase your skills! Whether you're a wizard at weaving undetectable malware or a mastermind in sophisticated defenses, this is your stage. Demonstrate your capabilities to a global audience, including potential employers and industry leaders.

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 12:30-12:59 PDT

Title: Manufacturing- Lessons Learned, Lessons Taught
When: Saturday, Aug 10, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Manufacturing continues to be a top targeted sector by cyber threat actors, especially by ransomware. Dragos 2023 Year In Review showed that 70% of all ransomware victims were manufacturers. The Global Resilience Federation Ransomware Report shows very similar figures. There are some specific elements that make manufacturing a particularly attractive target for ransomware such as the lack of network security and segmentation, IT compromise that often leads to operational disruption (even if there is not OT network intrusion), manufacturing having tight margins, a lack of a compliance regime, and organizational size all contributing. Manufacturing continues to be a top targeted sector by cyber threat actors, especially by ransomware. Dragos 2023 Year In Review showed that 70% of all ransomware victims were manufacturers. The Global Resilience Federation Ransomware Report shows very similar figures. There are some specific elements that make manufacturing a particularly attractive target for ransomware such as the lack of network security and segmentation, IT compromise that often leads to operational disruption (even if there is not OT network intrusion), manufacturing having tight margins, a lack of a compliance regime, and organizational size all contributing.

While manufacturing as a whole lags many other critical infrastructure sectors in aspects of cyber security there is a category that manufacturing has consistently led other industry verticals in, automation and device connectivity in the operational technology domain. Manufacturer's OT network environments increasingly are set up as a network or hyper connected IIoT devices, where all data goes to the cloud and often comes back from the cloud to offer changes, and all participants have access into the OT network domain allowing manufacturing to push the boundaries of what products are technically possible, what production efficiencies are possible, and how OT environments can scale as never before.

This has obviously come with downside risks that manufacturers are only now beginning to grapple with and to make meaningful changes to better protect their networks and the gains they have made. Their growing pains can serve as roadmap of what to do and what not to do as many other OT intensive industry verticals are moving very quickly into similar use cases.

SpeakerBio: Tim Chase, Program Director at Global Resilience Federation (GRF)

Tim Chase is a Program Director with the Global Resilience Federation (GRF), he brings nearly a decade of collective defense and intelligence analysis experience to the communities he leads. He has worked across various critical infrastructure sectors in several information sharing communities. He leads the Manufacturing Information Sharing and Analysis Center (MFG-ISAC) where he engages members to facilitate cyber security success for manufacturers and their support ecosystem. The MFG-ISAC facilitates the exchange of cyber threat intelligence, vulnerabilities, and mitigation strategies while fostering member collaboration with other key sectors and government agencies to respond and prevent critical threats and incidents.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 14:30-14:59 PDT

Title: Mapping the Landscape: Top 10 Cybersecurity Trends in Critical Infrastructure for 2024
When: Friday, Aug 9, 14:30 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

In recent years, we have witnessed a surge in attacks aimed at critical infrastructure, varying widely in scope and impact depending on the region. While the definition of critical infrastructure differs by country, it typically encompasses essential sectors such as oil, natural gas, water, power, and manufacturing. The ramifications of these attacks are complex and often unpredictable.

To gain a clearer understanding of the state of critical infrastructure globally, starting in 2023, we will annually survey 300 CISOs or security directors across different countries in this sector. We will share the data-driven insights to offer a detailed examination of the current conditions and challenges faced by these crucial systems. By comparing trends across different years, countries, and industries, our goal is to enhance the security and resilience of critical infrastructures worldwide.

SpeakerBio: Mars Cheng, Threat Research Manager, PSIRT and Threat Research at TXOne Networks Inc

Mars Cheng (@marscheng_) leads TXOne Networks' PSIRT and Threat Research Team as Threat Research Manager, coordinating product security initiatives and threat research efforts. He is also the Executive Director for the Association of Hackers in Taiwan (HIT/HITCON) and General Coordinator of HITCON CISO Summit 2024, facilitating collaboration between enterprises and the government to bolster the cybersecurity landscape. Mars is a frequent speaker and trainer at numerous prestigious international cybersecurity conferences and has presented over 50 times, including Black Hat USA/Europe/MEA, RSA Conference, DEF CON, CODE BLUE, FIRST, HITB, HITCON, Troopers, NOHAT, SecTor, SINCON, ROOTCON, ICS Cyber Security Conference Asia and USA, CYBERSEC, CLOUDSEC, VXCON, and many others. His expertise spans ICS/SCADA systems, malware analysis, threat intelligence and hunting, and enterprise security. Mars has made significant contributions to the cybersecurity community, including authoring more than ten CVE-IDs and publishing in three SCI journals on applied cryptography. Mars has successfully organized several past HITCON events, including HITCON CISO Summit 2023, HITCON PEACE 2022, HITCON 2021, and HITCON 2020.

Return to Index - Add to Google - ics Calendar file

VMV - Friday - 16:15-16:59 PDT

Title: Maricopa County -Preparing for the 2024 Elections Cycle
When: Friday, Aug 9, 16:15 - 16:59 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

A comprehensive presentation on the evolving landscape of elections in Maricopa County since the continuous 2020 Presidential Election. We will begin with an introduction to Maricopa County, highlighting its demographic and political significance. Following this, we will outline the key dates and events in the 2024 election calendar, ensuring you are well-prepared for the upcoming electoral cycle. Delving into the voting methods available to Maricopa residents, including in-person, mail-in, and early voting options, emphasizing accessibility and convenience we will explore major changes implemented since the 2020 elections. Focusing on improvements in technology, security, and voter engagement, and reflect on the critical lessons learned from the 2022 elections that have shaped current practices and policies.Looking ahead to the 2024 elections, we will provide an overview of anticipated challenges and opportunities for voter participation. Security is paramount, and we will detail the physical security enhancements made at the voting tabulation center, as well as the strategies and protocols in place for effective coordination with law enforcement. Understanding and mitigating insider threats is essential, and we will cover the measures taken to protect against internal risks. We will also review recent statutory changes affecting elections and their implications for voters and election officials. Finally, we will highlight the importance of social media training for election staff to combat misinformation and engage with the community effectively. Join us for this informative session to gain a deeper understanding of Maricopa County's election processes and the continuous efforts to enhance transparency, security, and voter confidence.

Speakers:Nate Young,Jason Butryn

SpeakerBio: Nate Young

Nate Young is the Chief Information Officer at the Maricopa County Recorders & Elections departments. Nate has worked with Maricopa County since 2018 and is current responsible for the County Document Recordation functions and Elections Technology operation processes. Nate actively participates in Elections and Technology committees and helped represent the County during the Arizona Senate Audit of the 2020 Presidential Election by the Cyber Ninjas.

SpeakerBio: Jason Butryn

Jason Butryn is the Information Security Officer (ISO) for the Maricopa County Recorder and Elections. He has been in Information Technology for the past 20 years and other than working for the San Manuel Band of Mission Indians to start his career, he has been working in the public sector his entire career. He started out in infrastructure engineering and management and has pivoted his career to Information Security.

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 16:30-16:59 PDT

Title: Master Splinter's initial physical access dojo: Storytelling of a complex adversarial attack
When: Friday, Aug 9, 16:30 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Storytelling of a highly complex Red Team with multiple initial accesses only with Social Engineering. could anyone do it? Yes.

Under the format of Storytelling this presentation aims to take attendees first person through a RedTeam service with multiple initial accesses with 100% Social Engineering. How to present critical vulnerabilities in a public way without exposing the target company? This live comic will show us how, through one of its protagonists and with practical examples made with the attendees themselves. How does a professional Social Engineering unit work? What are the roles and tasks? How to emulate the reach of a cybercriminal gang in less than three weeks? This dojo aims to show the methodologies and techniques applied in the field to obtain relevant findings, even reaching critical infrastructure without raising alerts and in an extremely limited time. From the first meeting with the client, information gathering, vector selection, exploitation, pretexting to the physical intrusion, even reaching the datacenter. We will demonstrate how luck is no longer an element to consider when your work is SE from Monday to Friday and you have to perform this type of service every month.

SpeakerBio: Daniel Isler, Team Leader, Fr1endly RATs at Dreamlab Technologies Chile

Daniel has a bachelor's in arts of Representation. With certifications in Social Engineering, Red Team and OSINT. Team Leader of Fr1endly RATs, the Social Engineering unit at Dreamlab Technologies Chile. Specializing and developing techniques and methodologies for simulations of Phishing attacks, Vishing, Pretexting, Physical Intrusions and Red Team.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 12:20-12:50 PDT

Title: Maturing Your Application Security Program
When: Saturday, Aug 10, 12:20 - 12:50 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

After working with over 400 companies on their application security programs the most common question I receive is “what’s next?”. They want to know how to mature their programs, and when they look at the maturity models available, they find them intimidating and so far beyond their current maturity level that they feel impossible. In this talk I will take you through 3 common AppSec program maturity levels I have encountered over the years, with practical and actionable next steps you could take immediately to improve your security posture.

SpeakerBio: SheHacksPurple

Tanya Janca, also known as SheHacksPurple, is the best-selling author of ‘Alice and Bob Learn Application Security’. She also is the head of education and community at Semgrep, running their online community and academy which both revolve around teaching everyone to create secure software. Tanya has been coding and working in IT for over twenty five years, won countless awards, and has been everywhere from startups to public service to tech giants (Microsoft, Adobe, & Nokia). She has worn many hats; startup founder, pentester, CISO, AppSec Engineer, and software developer. She is an award-winning public speaker, active blogger & streamer and has delivered hundreds of talks and trainings on 6 continents. She values diversity, inclusion and kindness, which shines through in her countless initiatives.

Advisor: Nord VPN, Katilyst, ICTC PAC

Founder: We Hack Purple, WoSEC International (Women of Security), OWASP DevSlop, #CyberMentoringMonday

Faculty: IANS Research

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 14:00-14:59 PDT

Title: MCPA x BIC x CAPT Virtual National Service Panel 2024
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

National Service and Cybersecurity: Bridging the Gap Across Experiences

In an increasingly interconnected world, cybersecurity stands at the forefront of national security and defense. This panel brings together a diverse group of veterans, federal civilians, and actively serving soldiers to delve into the critical intersection of national service and cybersecurity. Through their unique perspectives and experiences, the panelists will shed light on how their respective roles play a vital part in protecting national interests and addressing the ever-evolving landscape of cyber threats.

Our panel aims to underscore each group's indispensable contributions to the cybersecurity field, from veterans' strategic and operational insights to active service members' hands-on expertise and federal civilians' policy and management perspectives. By attending, you will gain valuable insights into the synergies between these roles and the pivotal role of collaboration in fortifying national security.

Join us for a compelling discussion on the profound impact of national service on cybersecurity, the challenges encountered by each group, and the vast opportunities for future collaboration to fortify our digital infrastructure.

Speakers: Sydney Johns,Nikkia Henderson,Manvell Lessane,Dr. William (Bill) Butler,Dr. Juel Tillman

SpeakerBio: Sydney Johns, Phd Student & Artificial Intelligence Researcher at Johns Hopkins Human Language Technology Center of Excellence

Sydney Johns is an Artificial Intelligence Researcher at the Johns Hopkins Human Language Technology Center of Excellence. She was previously a Computer Engineer in the Army C5ISR Research and Technology Integration Directorate and has worked for the JHU Applied Physics Laboratory and Northrop Grumman.

SpeakerBio: Nikkia Henderson, Program Operations Lead

Nikkia Henderson is a 14 year tenured federal government employee. In her current role she is a Senior Advisor at the Cybersecurity Infrastructure Security Agency (CISA). She serves a Cyber Supply Chain Risk Management (C-SCRM) Strategy and Governance Program lead, within CISA’s Cybersecurity Division. Ms. Henderson is also the President of the Women in Cybersecurity Mid Atlantic Affiliate, where she serves as a "cybHERprenuer" who is passionate about helping Cybersecurity/IT professionals define their vision, mission, and federal career path. In this session, Ms. Henderson shares her journey into a federal cyber career. She will highlight her challenges as well as milestones that catapulted her to where she is today!

SpeakerBio: Manvell Lessane, Cybersecurity Professional

With over two decades of dedicated service in the federal government, Manvell Lessane is a seasoned cybersecurity professional known for his robust expertise across multiple domains of information technology, cybersecurity program management, contracting, and acquisitions.

Manvell Lessane's journey began at the age of 16, when he participated in the Mayor's Youth Program in Washington, DC. This early experience ignited a passion for public service and technology, paving the way for a prestigious career in cybersecurity and IT within the federal landscape.

Throughout his career, Manvell Lessane has worn many hats, demonstrating a versatile command over IT and cybersecurity program management. His solid grasp of contracting and acquisitions has further underscored his ability to navigate and streamline complex governmental processes.

Through his expansive career, Manvell Lessane has continuously driven developments in cybersecurity policies and IT program management strategies, fostering a more secure and efficient governmental infrastructure.

Manvell Lessane embodies a commitment to excellence, bringing a wealth of knowledge, leadership, and innovation to every team and project. His journey is a testament to the impact of dedication and lifelong learning in the ever-evolving landscape of cybersecurity and IT management.

Passionate about the future of cybersecurity and public service, Manvell Lessane continues to be a vital asset in fortifying the digital defenses of the federal government, ensuring the safety and integrity of critical information systems nationwide.

Manvell Lessane holds an impressive array of academic credentials, including: - Master of Business Administration (MBA) - Master's in Communication Technology - Master’s degree in Law with a specialization in Cybersecurity Law and Policy

In recognition of his skills and dedication, Manvell Lessane has achieved several high-level certifications: - Project Management Professional (PMP) - Certified Information Security Manager (CISM) - Federal Acquisition Certification for Contracting Officer’s Representative (FAC-COR II) - Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) with a specialization in IT

SpeakerBio: Dr. William (Bill) Butler, Vice President Cyber Science Outreach and Partnerships at Capitol Technology University

Dr. William (Bill) Butler is the Vice President of Cyber Science Outreach and Partnerships at Capitol Technology University. Beginning in 2021, he served as Vice President of Academic Affairs and Cybersecurity Chair for 8 years at Capitol Tech. Earlier in his career, he worked as a network engineer and consultant in the networking and I.T. industries for over 30 years. Dr. Butler also served as a joint qualified communications information systems officer in the U.S. Marine Corps and retired as a Colonel with 30 years of service (active and reserve). He is very active in various working groups such as the National Institute of Standards and Technology Cloud Computing Security Forum Working Group (NIST CCSFWG), Cloud Security Alliance (CSA) Big Data and Mobile Computing Working Group, and the National Cyber Watch Center Curriculum Taskforce and the National Cybersecurity Student Association Advisory Board. Dr. Butler holds degrees from Brenau University, Marine Corps University, U.S. Army War College, National Defense University, University of Maryland, and Capitol Technology University. He earned his DSc in cybersecurity at Capitol in 2016, with a Dissertation titled "PRESERVING CELLPHONE PRIVACY - COUNTERING IMSI CATCHERS."

SpeakerBio: Dr. Juel Tillman, Service Member & Cybersecurity Professional

First Sergeant Juel Tillman has served in the armed forces for over 23 years with three branches of service (United States Marine Corps, United States Army, and the Delaware National Guard). While serving, First Sergeant Tillman has deployed nine times under three campaigns (Operation Iraqi Freedom, Operation Enduring Freedom, and Operation Inherent Resolve)and has received 19 medals, Gung Ho Award (Marine Corps), Distinguished Honor Grade (Senior Leadership Course), Distinguish Leadership awards, SBI Duncan award, letters of Appreciation Awards, Certificates of War Time Service, and Certificates of Achievement, based on performance, leadership, and expertise in heavy equipment operations, network operations, network security, tactical security, and field construction. While serving, First Sergeant Tillman completed Doctorate Degree, Three master’s degrees, bachelor’s degree, and associate’s degree.

Return to Index - Add to Google - ics Calendar file

PLV - Saturday - 12:30-12:50 PDT

Title: Measuring the international balance of trade in Internet bandwidth: introducing Netflow to Ministries of Finance
When: Saturday, Aug 10, 12:30 - 12:50 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

Internet bandwidth, or transit, the thing that people pay for when they “connect to the Internet,” is largely transnational, and is balanced by substantial transborder flows of capital. As the Internet becomes our primary mode of communication, the international financial impact of trade in Internet bandwidth itself becomes a substantial risk for net-consumer countries like India and the United Arab Emirates, and a substantial opportunity for net-exporter countries like the Netherlands and Brazil. Governments are beginning to recognize these risks and opportunities, and seeking to manage them in an informed and deliberate way, which requires instrumentation of flows of bandwidth which haven’t existed ubiquitously since prior to the 1992 privatization of the Internet and dissolution of the centralized Internet backbone. This talk looks at the mechanisms and efforts underway in intergovernmental treaty organizations to coordinate harmonized and repeatable technical mechanisms of bandwidth measurement.

SpeakerBio: Bill Woodcock, Executive Director at Packet Clearing House

Bill Woodcock is the executive director of Packet Clearing House, the intergovernmental treaty organization that supports the operation of critical Internet infrastructure, including Internet exchange points and the core of the domain name system. Since entering the Internet industry in 1985, Bill has helped establish more than three hundred Internet exchange points. In 1989, Bill developed the anycast routing technique that now protects the domain name system. In 1998 he was one of the principal drivers of California 17538.4, the world’s first anti-spam legislation. Bill was principal author of the Multicast DNS and Operator Requirements of Infrastructure Management Methods IETF drafts. In 2002 he co-founded INOC-DBA, the security-coordination hotline system that interconnects the network operations centers of more than three thousand Internet Service Providers and Security Operations Centers around the world. And in 2007, Bill was one of the two international liaisons deployed by NSP-Sec to the Estonian CERT during the Russian cyber-attack. In 2011, Bill authored the first survey of Internet interconnection agreements, as input to the OECD’s analysis of the Internet economy. Bill served on the Global Commission on the Stability of Cyberspace and on the Commission on Caribbean Communications Resilience. He's on the board of directors of the M3AA Foundation, and was on the board of the American Registry for Internet Numbers for fifteen years. Now, Bill’s work focuses principally on the security and economic stability of critical Internet infrastructure.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 15:00-15:45 PDT

Title: Measuring the Tor Network
When: Saturday, Aug 10, 15:00 - 15:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Millions of people around the world use Tor every day to protect themselves from surveillance and censorship. While the Tor Browser and its protocol are widely known, the backbone of the Tor ecosystem, its extensive network of volunteer relays, is often subject to speculation and misinformation. The Tor Project is dedicated to supporting this network and fostering a vibrant, diverse community of relay operators.

This talk will focus on our efforts to maintain a healthy network and community, and detect and mitigate attacks -- all with the help of metrics and analysis of usage patterns. By illustrating how we collect safe-enough metrics for an anonymity network, we will offer insights into how we identify unusual activity and other noteworthy events on the network. We will also discuss our ongoing strategies for addressing current and future network health challenges.

If you are interested in understanding the inner workings of the Tor network and its relay community and how we keep this vital ecosystem running, this talk is for you.

1. Network Health Team wiki: link
2. Two blog posts on Tor network health: link link
3. Collector (where we archive all network data sets): link
4. Paper by Rob Jansen et al. on incentives schemes for relays on the Tor network, "Recruiting New Tor Relays with BRAIDS": link
5. Broader blog post about research papers on incentive for Tor relays: link
6. Research paper by NRL proposing how to measure relay performance in a way that resists attempts to lie about relay speed: link
7. Our plan to change how we collect, store and serve Tor network data (discussion from our bug tracker): link
8. Performance measurements over the Tor Network: link
9. Onionperf is the tool we use to measure performances from different locations across the globe: link
10. The number of relays on the network by relay flags: link
11. Documentation about reproducible metrics: link

Speakers: Silvia Puglisi,Roger Dingledine

SpeakerBio: Silvia Puglisi, Lead, Network Health at Tor Project

Silvia Puglisi is a Systems Engineer and Privacy Researcher based in Barcelona, EU. She currently leads the network health team at the Tor Project, focusing on maintaining the stability, performance, and security of the Tor network. Silvia is also an O'Reilly author and previously worked at Google for several years. She was part of the Information Security Group at the Department of Telematics Engineering, Universitat Politècnica de Catalunya (UPC), where she earned her Ph.D. Additionally, she has served as an adjunct professor at the Universitat Oberta de Catalunya (UOC).

SpeakerBio: Roger Dingledine, Co-Founder and Original Developer at Tor Project

Roger Dingledine is co-founder and original developer of the Tor Project, a nonprofit that develops free and open source software to protect people from tracking, censorship, and surveillance online. Roger works with journalists and activists on many continents to help them understand and defend against the threats they face, and he is a lead researcher in the online anonymity field. EFF picked him for a Pioneer Award, and Foreign Policy magazine chose him as one of its top 100 global thinkers.

BBV - Saturday - 17:30-17:59 PDT

Title: Meet the PortSwigger Research team (Q/A)
When: Saturday, Aug 10, 17:30 - 17:59 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

Meet the minds behind a decade of acclaimed web security research. Whether you'd like to query our thoughts on technical matters or career decisions, share something cool you've found, flood us with Burp Suite feature requests, or simply say hi, this is your chance! We're also giving three presentations at DEF CON so if you'd like to treat this as an extended Q&A for those, that's cool too. Please note this session may be chaotic.

Speakers: Martin Doyhenard,James "albinowax" Kettle,Gareth Heyes

SpeakerBio: Martin Doyhenard, Security Researcher at Portswigger

Martin Doyhenard is a Security Researcher at Portswigger, known for exploiting HTTP servers and web applications. Over the past few years he has presented his findings in multiple top security conferences including BlackHat, DEFCON, RSA, EkoParty, Hack in The Box and Troopers.

His latest work includes discovering HTTP Response Smuggling techniques and exploiting SAP’s Inter-Process Communication service - compromising more than 200 thousand companies in the world.He’s also passionate about low level reverse engineering and testing his skills in online CTFs.

SpeakerBio: James "albinowax" Kettle, Director of Research at PortSwigger

James 'albinowax' Kettle is the Director of Research at PortSwigger, the makers of Burp Suite. He's best known for his HTTP Desync Attacks research, which popularised HTTP Request Smuggling. James has extensive experience cultivating novel attack techniques, including web cache poisoning, browser-powered desync attacks, server-side template injection, and password reset poisoning. James is also the author of multiple popular open-source tools including Param Miner, Turbo Intruder, and HTTP Request Smuggler. He is a frequent speaker at numerous prestigious venues including both Black Hat USA and EU, OWASP AppSec USA and EU, and DEF CON.

SpeakerBio: Gareth Heyes, Researcher at PortSwigger

PortSwigger researcher Gareth Heyes is probably best known for smashing the AngularJS sandbox to pieces and creating super-elegant XSS vectors. He is the author of JavaScript for hackers. In his daily life at PortSwigger, Gareth can often be found creating new XSS vectors, and researching new techniques to attack web applications. He has a keen interest in hacking CSS to do wonderful, unexpected things and can often be seen experimenting with 3D pure CSS rooms, games and taking markup languages to the limit on his website. He's also the author of PortSwigger's XSS Cheat Sheet. In his spare time, he loves writing new BApp extensions such as Hackvertor.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 08:00-17:59 PDT

Title: Merch (formerly swag) Area Open -- README
When: Friday, Aug 9, 08:00 - 17:59 PDT
Where: LVCC West/Floor 2/W212 - Map

Description:

All merch sales are USD CASH ONLY. No cards will be accepted.

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

Note that the closing hours here are **when sales must have ended**. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 09:00-14:59 PDT

Title: Merch (formerly swag) Area Open -- README
When: Saturday, Aug 10, 09:00 - 14:59 PDT
Where: LVCC West/Floor 2/W212 - Map

Description:

All merch sales are USD CASH ONLY. No cards will be accepted.

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

Note that the closing hours here are **when sales must have ended**. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

Return to Index - Add to Google - ics Calendar file

MISC - Thursday - 08:00-17:59 PDT

Title: Merch (formerly swag) Area Open -- README
When: Thursday, Aug 8, 08:00 - 17:59 PDT
Where: LVCC West/Floor 2/W212 - Map

Description:

All merch sales are USD CASH ONLY. No cards will be accepted.

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

Note that the closing hours here are **when sales must have ended**. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 16:30-17:25 PDT

Title: Meshtastic Adventures: Triumphs, Tribulations, and Total Mesh-ups.
When: Friday, Aug 9, 16:30 - 17:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

The submitted talk will include the intro technical details of Meshtastic. However, the majority of this talk is aimed at the planning, mapping, business and personal contacts of site owners (and the headaches involved), success and failures of our project and node builds. As well as some advanced settings to hide your node deployments in some creative ways. More of a how to build out your mesh network rather than a technical deep dive.

SpeakerBio: m1ddl3w4r3

For the past six years, I've been a Defcon attendee and RFCTF competitor. My passion for RF is only rivaled by my love for teaching people "stuff and things" – it's a technical term, trust me. I'm a Co-Organizer for a local meetup for hackers in my area called CAH (Central Arkansas Hackers), where we bond over shared interests and a collective lack of sleep. I've also been creating RF challenges at a local CTF (Jolt Hackathon) for the past few years, turning innocent students and professionals into RF hacking aficionados, or at least into people who know how to spell RF. This would be my first Defcon talk, and I'd love the chance to dazzle (or at least mildly amuse) the audience with my antics.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 16:30-17:59 PDT

Title: Meshtastic Meetup
When: Friday, Aug 9, 16:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Come learn about Meshtastic, the long-range, low-power, encrypted off-grid messaging protocol. We'll be setting up our Meshtastic Nuggets, going over the setup options, and exploring the advanced options that make Meshtastic more useful. We'll cover setting encryption, choosing a device role, and connecting over serial, web, and bluetooth. We'll also look at some of the optional modules, like broadcasting sensor telemetry data or adding a GPS.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 16:30-17:59 PDT

Title: Meshtastic Meetup
When: Saturday, Aug 10, 16:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Come learn about Meshtastic, the long-range, low-power, encrypted off-grid messaging protocol. We'll be setting up our Meshtastic Nuggets, going over the setup options, and exploring the advanced options that make Meshtastic more useful. We'll cover setting encryption, choosing a device role, and connecting over serial, web, and bluetooth. We'll also look at some of the optional modules, like broadcasting sensor telemetry data or adding a GPS.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 12:30-13:30 PDT

Title: Mexicans Together - Un vistazo a recientes investigaciones de nuestros dos equipos globales
When: Friday, Aug 9, 12:30 - 13:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Esta plática abordará detalles sobre tres investigaciones recientemente realizadas por el equipo de respuesta a incidentes (GERT) y el equipo de investigación (GReAT). La plática será impartida por María Isabel (GReAT) y Ashley Hiram (GERT) mostrando las investigaciones hechas en conjunto con la finalidad de brindar diferentes perspectivas, así como resaltar la colaboración y resultados de ambos equipos, resaltando que una de ellas nos permitió añadir una sub-técnica al MITRE ATT&CK.

Las investigaciones a mostrar son conocidas como:

- NKAbuse: Malware que utiliza Blockchain para su C2.
- LockBit 3.0 Builder: Capacidades adicionales a LockBit.
- Grandoreiro: Campañas de alcance global.

We will talk about three investigations recently conducted by the Incident Response Team (GERT) and the Investigation Team (GReAT). The talk will be given by María Isabel (GReAT) and Ashley Hiram (GERT) showing the research done together with the purpose of providing different perspectives, as well as highlighting the collaboration and results of both teams, highlighting that one of them allowed us to add a sub-technical to MITRE ATT&CK.

The investigations to be shown are known as:

- NKAbuse: Malware that uses Blockchain for your C2.
- LockBit 3.0 Builder: Additional capabilities to LockBit.
- Grandoreiro: Global reach campaigns.

Speakers:
Ashley Hiram M.,Isabel Manjarrez

SpeakerBio:
Ashley Hiram M., Incident Response Specialist (GERT)

I currently work as an Incident Response Specialist on the GERT team, I have 5-6 years of experience performing digital forensics, Malware Analysis and Reversing.

I have collaborated on different Threat Intelligence and Threat Hunting projects.

Before dedicating myself to DFIR (Digital Forensics and Incident Response), I worked for 2 years as a Pentester in a well-known Mexican consulting company.

Certifications: GREM, GCFA, eCTHP, CHFI.

Actualmente me desempeño como Especialista en Respuesta a Incidentes en el equipo GERT, cuento con 5-6 años de experiencia realizando tanto forense digital, así como Análisis de Malware y Reversing.

He colaborado en diferentes proyectos de Threat Intelligence y Threat Hunting.

Previo a dedicarme a DFIR (Digital Forensics and Incident Response), laboré 2 años como Pentester en una conocida empresa de consultoría mexicana.

Certificaciones: GREM, GCFA, eCTHP, CHFI.

SpeakerBio: Isabel Manjarrez, Threat Researcher (GReAT)

I am currently part of the Global Research and Analysis team (GReAT). My activities include investigating the most active threat actors, tracking their movements and analyzing new implemented techniques. With bases in telecommunications and electronics, today I have more than five years of experience performing threat intelligence tasks.

Actualmente soy parte del equipo de Global de Investigación y Análisis (GReAT). Mis actividades incluyen investigar a los actores de amenaza más activos, seguir sus movimientos y analizar nuevas técnicas implementadas. Con bases en telecomunicaciones y electrónica, hoy cuento con más de cinco años de experiencia realizando tareas de inteligencia de amenazas.

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 12:30-12:59 PDT

Title: MFT: Malicious Fungible Tokens
When: Friday, Aug 9, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

In this technical talk, we will uncover a new aspect of NFTs: using them as attack vectors to relay C2 commands. Fingerprinting a system? Exfiltrating information? Encrypting and wiping data? Executing arbitrary commands? Of course! But with a dark twist: deployed NFTs are blockchain-backed assets immune to takedowns. Imagine having your own “immortal” C2 Server for less than $10 dollars in $ETH.

For this, we will introduce “mFT” an open-source tool that automates the creation of malicious payloads and provide sample harmless NFTs, allowing attendees to explore this novel attack vector on their own machines safely. This talk is the spiritual successor of "Everything is a C2 if you're brave enough".

Speakers: Cybelle Oliveira ,Mauro Eldritch

SpeakerBio: Cybelle Oliveira , CTI Malwarelandia

Cybelle Oliveira is a Cybersecurity Consultant, postgraduate in Cyber Threat Intelligence and Master's student in Cyber intelligence at the International Cybersecurity Campus of the University of Murcia, Spain. She has been involved in privacy and security activism for over 10 years and has presented talks at events around the world, including BSides LV, BSides SP, Girls Hack Village (DefCon), 8.8 Chile, Internet Freedom Festival, Radical Networks, Mozilla Festival, Roadsec, Cryptorave, among others. Cybelle is part of the Mozilla community and is the director of the Casa Hacker organization.

Cybelle Oliveira es Consultora de Ciberseguridad, postgraduada en Cyber Threat Intelligence y estudiante de Máster en Ciberinteligencia en el Campus Internacional de Ciberseguridad de la Universidad de Murcia, España. Ha estado involucrada en activismo de privacidad y seguridad durante más de 10 años y ha presentado charlas en eventos por todo el mundo, como BSides LV, BSides SP, Girls Hack Village (DefCon), 8.8 Chile, Internet Freedom Festival, Radical Networks, Mozilla Festival, Roadsec, Cryptorave, entre otros. Cybelle forma parte de la comunidad Mozilla y es directora de la organización Casa Hacker.

SpeakerBio: Mauro Eldritch, Founder at Birmingham Cyber Arms LTD

Mauro Eldritch is an Argentine hacker, founder of Birmingham Cyber Arms LTD and DC5411 (Argentina / Uruguay). He has spoken at various events, including DEF CON (10 times). He is passionate about Threat Intelligence and Biohacking.

Mauro Eldritch es un hacker argentino, fundador de Birmingham Cyber Arms LTD y DC5411 (Argentina / Uruguay). Habló en diferentes eventos incluyendo DEF CON (10 veces). Le apasiona la Inteligencia de Amenazas y el Biohacking.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 15:30-15:59 PDT

Title: Microhard? More like MicroEASY...to exploit...
When: Friday, Aug 9, 15:30 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Microhard is a Canadian-based company that specializes in long range "robust" radio equipment. They are used in SCADA environments, point-of-sale terminals, power utilities, and more. From a security standpoint, however, some of their products are anything but "robust". And they have a habit of hiding their vulnerability fixes behind intentionally vague release notes, which will make this even more fun! (No, I'm not bitter at all) Command injections and buffer overflows abound, as well as a lesson or two in the need for a "robust" secure development process.

SpeakerBio: Ricky "HeadlessZeke" Lawshae, Principal Security Researcher at Keysight

Ricky "HeadlessZeke" Lawshae is a Principal Security Researcher at Keysight with well over a decade of experience in the fields of vulnerability research, exploitation, reverse engineering, and network/hardware analysis. He has spoken at many conferences around the world including DEFCON (x5), Recon, and Toorcon. His work has been featured on Forbes, Wired, and Hackaday. These days, he mostly focuses on offensive IoT research.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 11:00-13:59 PDT

Title: Mind-Controlling Other Applications: An intro to intra-process hacking
When: Friday, Aug 9, 11:00 - 13:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Classroom - Map

Description:

Learn from the ground up how to take over the execution of another process and make it do your bidding! This workshop teaches you the basic to intermediate levels of runtime intra-process hacking on Windows and POSIX systems covering injecting code into another process on windows (and an overview of how this could be done on a POSIX system), locating specific code within an application in a update resistant manner, hooking and redirecting code execution using several techniques, abusing error handlers to disguise code and an overview of mitigation strategies to protect apps from intra-process hacking.

SpeakerBio: ILOVEPIE

Ever since I found the only 3 books on programming in my elementary school's library I've been captivated by the logical and mathematical problems presented by the field of Computer Science and how the solutions to those problems can go wrong and be exploited. In high-school I discovered a zero day Denial Of Service exploit in all implementations of the Minecraft server at that time. I promptly proceeded to crash, what was at the time, the largest Minecraft server in the world (with permission). From there my interests drifted more towards cybersecurity, particularly with regards to video games. I wrote a tool to dump and partially deobfuscate the RuneScape client while it was loading and have also written proof-of-concept hacks for several games and multiple game-server emulators. I am currently a maintainer for opentypejs/opentype.js (a font library in pure JS) and SABRE-JS/SABRE.js (a GPU accelerated subtitle renderer for the most advanced subtitle format in the world).

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 12:00-12:50 PDT

Title: Mining for Abandoned Gold in DNS
When: Friday, Aug 9, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Ascension - Map

Description:

In the cloud computing landscape, the ease of resource allocation by cloud providers contrasts sharply with traditional computing's constraints, turning IPv4 addresses into digital assets with multiple tenancies. Our presentation explores the "Dangling DNS" phenomenon—active DNS records pointing to IP addresses uncontrolled by the domain owner, creating potential security vulnerabilities.

We will unravel the persistence of IP address-based authentication and authorization practices on the internet and discuss methods to enhance the credibility of these dangling DNS entries, including the acquisition of x.509 certificates. The implications are significant, offering avenues for commandeering these entries for Command and Control (C2) operations or crafting phishing emails capable of circumventing standard email security frameworks.

Following the foundational discussion, our presentation will delve into analysis of dangling DNS entries discovered in live environments. We will discuss the widespread occurrence of dangling DNS entries, identifying the cloud providers where they are most frequently found. Furthermore, we will delve into specific case studies, presenting particularly intriguing instances of dangling DNS entries to underscore their varied nature and potential implications.

A pivotal segment of our presentation introduces innovative methodologies for the identification of dangling DNS vulnerabilities. We will showcase "Paydirt," an open-source tool, written by the author, designed to unearth dangling DNS entries within cloud provider shared IP address space. Furthermore, we will unveil a tool at Defcon 2024, engineered to detect exploitable cloud IP addresses within Sender Policy Framework (SPF) entries, a critical vector for executing sophisticated spear-phishing campaigns.

Our presentation aims not only to highlight the security challenges posed by the transient nature of cloud-assigned IP addresses but also to equip the cybersecurity community with simple actionable strategies to fortify their defenses against these threats.

SpeakerBio: Matt Pawloski
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: Misinformation, Disinformation, and Malformation in 2024
When: Saturday, Aug 10, 17:00 - 17:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

This panel will cover the misinformation, disinformation, and malinformation that we are seeing across different mediums prior to the upcoming presidential election. Join us for an all star panel of misinformation, disinformation, and malformation experts discuss the threats they are currently observing and what their biggest concerns are for the upcoming election. Audiences will also learn what kind of precautions are being taken and what individuals can do to prepare themselves and increase their media literacy and ability to identify information that actually has information integrity.

Speakers: Nicole Tisdale,Michael Moore,Nate Young,Jake Braun,Derek DelGaudio,Kendall Spencer

SpeakerBio: Nicole Tisdale

For fourteen years, Nicole Tisdale has served as a national security expert at The White House - National Security Council (NSC) and the U.S. Congress' House Committee on Homeland Security. She is a policy expert on cybersecurity, counterintelligence, foreign malign influence, disinformation, and election security. She founded Advocacy Blueprints, and authored Right To Petition, a guide to exercising the First Amendment right to advocate. Originally from Nettleton, MS, Nicole is a barred attorney and alumna of The University of Mississippi (BA, 2006; JD, 2009).

SpeakerBio: Michael Moore

After volunteering to be a poll worker, Michael Moore developed a passion for Election Security. He was the first Information Security Officer for the Maricopa County Recorder's office and is now the first Chief Information Security Officer for the Arizona Secretary of State.Michael believes it is only through effective federal, state, and local government partnerships, as well as assistance from trusted vendors that we can protect our democracy and fulfill our duty to the American voter. The greatest threats to elections are MDM and the resulting insider threat caused by radicalized citizens. The best protection against these threats is combatting lies with the truth, developing secure and resilient systems that prevent attacks whenever possible, allow for detections of compromise and facilitate accurate and rapid recovery. Michael has pushed forward these initiatives in his own organizations as well as across the Michael is an alumnus of Arizona State University with a B.S. in Mathematics and a B.A. in Education,CISSP, Certified Election Official (CEO) and Certified Public Manager (CPM).Elections community.

SpeakerBio: Nate Young

Nate Young is the Chief Information Officer at the Maricopa County Recorders & Elections departments. Nate has worked with Maricopa County since 2018 and is current responsible for the County Document Recordation functions and Elections Technology operation processes. Nate actively participates in Elections and Technology committees and helped represent the County during the Arizona Senate Audit of the 2020 Presidential Election by the Cyber Ninjas.

SpeakerBio: Jake Braun

Jake Braun was appointed by President Joseph Biden as Senior Advisor to the Department of Homeland Security in February of 2021 where he focuses on Management issues. He is also a lecturer at the University of Chicago Harris School of Public Policy. He works at the center of politics, technology and national security to advance the field of cyber policy. He is the author of Democracy in Danger: How Hackers and Activists Exposed Fatal Flaws in the Election System and has co-authored two award-winning and seminal works on election infrastructure cyber vulnerabilities. Mr. Braun has worked extensively on national security and finance issues throughout the U.S., Europe, Asia, Africa, Middle East and Latin America. Prior to joining

the University of Chicago Harris School of Public Policy faculty and Cambridge Global Advisers, Mr. Braun was appointed by President Obama as White House Liaison to the Department of Homeland Security (DHS) where he oversaw some of the most high profile public engagements executed at DHS. He was instrumental in the effort to gain passage in the European Parliament of the largest big data sharing agreement in history between the United States and the European Union. In addition, he designed and implemented a program to modernize the DHS cybersecurity workforce. Mr. Braun also oversaw stakeholder crisis communications for the White House during the 2010 Deep Water Horizon Gulf Oil Spill.Prior to his tenure as White House Liaison, Mr. Braun served on the Presidential Transition Team for the Obama Administration as Deputy Director for the National Security Agencies Review. In this capacity he oversaw agency review programs for all national security agencies including the State Department, DOD, DHS, CIA, USAID, etc. and guided policy assessments from their inception to the President-Elect's desk. Mr. Braun also designs and implements political campaigns in the U.S., Asia, Africa, Latin America and Europe. Before coming to Washington, Mr. Braun served as the National Deputy Field Director to the 2008 Obama for America Campaign, overseeing an effort that utilized the most sophisticated grassroots, social media and data analysis available.In addition to his role at Harris, Mr. Braun is co-founder of the DEF CON Voting Machine Hacking Village, in the President's Circle on the Chicago Council on Global Affairs, and a strategic advisor to the Department of Homeland Security and the Pentagon on cybersecurity. DEF CON is the largest hacker conference in the world and in cooperation with them he has co-authored two fundamental and critically acclaimed reports on election infrastructure cyber vulnerabilities, The DEF CON 25 and 26 Voting Village Reports.

SpeakerBio: Derek DelGaudio
No BIO available
SpeakerBio: Kendall Spencer

Kendall Spencer wears a variety of interesting hats on a day to day basis. As a professional athlete, he's represented the United States in competition globally. But he is also the first black antique and rare book dealer in the US. Specializing in American history, he uses his experiences in the book trade to address how we might learn from history and restore democracy. Currently he is a lawyer at Ropes & Gray LLP, where he specializes in technology, cybersecurity, and corporate transactions.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 14:00-15:45 PDT

Title: MITRE Caldera for OT
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W303 - Map

Description:

Caldera for Operational Technology (C4OT) is an extension to the open-source Caldera adversary emulation platform. Adversary emulation has long helped defenders of information systems exercise and improve their cyber defenses by using real adversary techniques. While Caldera has been out since 2021, C4OT was released September 2023. Specifically, C4OT exposes native OT protocol functions to Caldera. The initial release of C4OT supported three popular OT protocols (Modbus, BACnet, and DNP3). Since then, we have added support for two more protocols (IEC61850 and Profinet). Today, we are actively working on support for the space protocol GEMS. By utilizing Caldera and the C4OT plugins, end-users can emulate threat activity across both Enterprise and Operational networks with ease.

Speakers: Blaine Jeffries,Devon Colmer

SpeakerBio: Blaine Jeffries, Operational Technology Security Engineer at MITRE Corp

Blaine Jeffries is an Operational Technology Security Engineer at MITRE with a focus on defensive cybersecurity research, threat intelligence and adversary emulation. At MITRE, Blaine currently serves as a co-lead of Caldera for OT and supports a variety of DoD and government sponsors. Prior to joining MITRE, Blaine served in the US Air Force as a Cyberspace Operations Officer. Currently he holds degrees in Electrical Engineering and Cyberspace Operations.

SpeakerBio: Devon Colmer, Cybersecurity Engineer, Critical Infrastructure Protection Innovation Center at MITRE Corp

Devon Colmer is a Cybersecurity Engineer in MITRE's Critical Infrastructure Protection Innovation Center, working principally in OT adversary emulation and detection engineering. Prior to joining MITRE, Devon served as a Submarine Officer in the US Navy. He has led the development of OT plugins for MITRE's adversary emulation platform, Caldera, and is currently researching a common data model for OT protocols.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 10:00-11:45 PDT

Title: MITRE Caldera
When: Saturday, Aug 10, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W308 - Map

Description:

MITRE Caldera is a scalable, automated adversary emulation, open-source cybersecurity platform developed by MITRE. It empowers cyber practitioners to save time, money, and energy through automated security assessments. Caldera not only tests and evaluates detection/analytic and response platforms, but it also provides the capability for your red team to perform manual assessments with computer assistance. This is achieved by augmenting existing offensive toolsets. The framework can be extended to integrate with any custom tools you may have. The development team behind the platform is a group of red teamers, software developers, exploit writers, cyber threat analysts, AI researchers, cybersecurity engineers, and computer scientists. They all pursue the common goal of building a premier adversary emulation platform for our security defenders around the world.

Speakers: Mark Perry,Rachel Murphy

SpeakerBio: Mark Perry, Lead Applied Cyber Security Engineer at MITRE Corp

Mark Perry is a Lead Applied Cyber Security Engineer at MITRE Corp, where he specializes in adversary emulation and work development. With a robust background in infrastructure and cyber security frameworks, Mark brings extensive expertise to his role, focusing on fortifying systems against sophisticated cyber threats. He has worked on projects involving adversary emulation, red teaming, cyber threat intelligence, and software development. Mark also leads development and delivery of Caldera workshops, providing participants with practical, hands-on training utilizing cybersecurity techniques. Additionally, he actively promotes Caldera's benefactor program, fostering community support and engagement to further the development of cybersecurity tools and resources. Outside of his professional endeavors, Mark enjoys traveling and is a supercar enthusiast.

SpeakerBio: Rachel Murphy, Cyber Security Engineer at MITRE Corp

Rachel Murphy is a Cyber Security Engineer at MITRE Corp. She has a B.S. in Mechanical Engineering and prior to joining MITRE, she worked as a mechanical engineer at NASA performing thermal analysis for the International Space Station at Johnson Space Center in Houston, TX. Rachel has worked on projects in adversary emulation, red teaming, cyber threat intelligence, and software development. Part of this work includes supporting Caldera's research in artificial intelligence, developing Caldera workshops like this one, and promoting Caldera's benefactor program. She has also served as a red team operator for MITRE Engenuity's ATT&CK Evaluations.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 10:00-10:45 PDT

Title: Mobile Mesh RF Network Exploitation: Getting the Tea from goTenna
When: Friday, Aug 9, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

False sense of security in devices that guarantee security is worse than no security at all. One device used by personnel who require communication security is goTenna Pro radio that creates an "off-the-grid" encrypted mobile mesh network.This network does not require any traditional cellular or satellite infrastructure and they may be found locally in your community. The datasheet says it is using AES-256 encryption. Has anyone bothered to verify that it is being implemented in the most secure manner? We examined this device and found that it was possible to fingerprint and track every off-the-grid message regardless of encryption. We also identified vulnerabilities that result in interception and decryption of the most secure encryption algorithm AES-256 as well as injection of messages into the existing mesh network. We don't just trust what datasheets say, we verify it for you. We will explain our testing methodologies and demonstrate exploitation in a live demo. We will discuss the operational implications of these vulnerabilities and safe ways of using these devices that decrease the chance of a compromise. The tools developed as part of this research will be released open-source to inform what was possible to inspire future research against similar devices. We will discuss how we worked with goTenna to remedy these issues.

Speakers:Erwin Karincic,Woody

SpeakerBio: Erwin Karincic

Erwin is an experienced security researcher specializing in both hardware and software reverse engineering, binary analysis, and exploit development across a range of processor architectures. He has notable experience in implementing complex Radio Frequency (RF) waveforms using Software Defined Radios (SDRs) for cybersecurity applications, complemented by his proficiency in designing, simulating, and fabricating antennas tailored for such applications. His past work includes extensive TCP/IP networking experience, designing worldwide secure communication systems. Erwin holds a number of prestigious certifications, including OSCP, OSCE, OSWE, OSEE, and CCIE Enterprise Infrastructure.

SpeakerBio: Woody

Woody thinks Linux is a member of the Charlie Brown gang who can lift heavy things but not always spell them. He has had some success with RF exploits in the past with the first ever goTenna exploit talk in the RF wireless village as well as the first attack against Ford Raptor key fobs with RaptorCaptor exploit. Woody's unique background, familiar to some, gives him a creative aspect to the impact of goTenna Pro research in the physical and RF world. Woody is also a staff member in the RFHacker Sanctuary, a member of Security Tribe, and has appeared on a few episodes of Hak5 describing novel device attacks.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 12:00-12:50 PDT

Title: Modern Red Teaming: macOS, K8s, and Cloud
When: Friday, Aug 9, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

You are targeting a modern organization, but new to you, the target environment has no Windows. You scour the internet for guidance, and find the results insufficient. You begin to think, “Progress will not happen until there is new maintainer.”

This talk presents a set of techniques for hacking environments built on macOS, Kubernetes, and cloud (AWS). These techniques are accompanied by anecdotes of adventures in Red Teaming. Attendees will learn new tricks for initial access, lateral movement, and persistence in modern non-Windows environments.

Speakers: Chris Gates,int eighty (of Dual Core)

SpeakerBio: Chris Gates
No BIO available
SpeakerBio: int eighty (of Dual Core)
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 14:00-15:50 PDT

Title: Modifying Impacket for Better OpSec
When: Friday, Aug 9, 14:00 - 15:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Operational security (OpSec) is a cornerstone in red teaming, necessitating continuous refinement of tools and techniques to avoid detection. This workshop is designed for new red team operators and individuals seeking to enhance their offensive capabilities. It focuses on customizing the Impacket toolset—a collection of Python classes for working with network protocols—to improve OpSec during engagements.

Impacket tools such as wmiexec, smbexec, and secretsdump are staples in the toolkit of any red teamer due to their versatility and power in gaining access and extracting sensitive data from Windows environments. However, their detectability has increased as defensive measures have become more sophisticated. This session proposes modifications to these tools to reduce their footprint and evade modern security defenses.

Participants will explore various customization strategies, including altering network signatures, timing attacks to evade detection, and integrating stealthier authentication methods. Practical exercises will guide attendees through the process of modifying the Impacket scripts, demonstrating how these changes can significantly enhance operational security in simulated environments.

SpeakerBio: Ryan O'Donnell, Senior Offensive Security Engineer at Microsoft

Ryan O'Donnell is an Offensive Security Engineer at Microsoft. Over the last 13+ years, Ryan has been performing Penetration Tests, Red Team assessments, and Incident Response investigations. Ryan has conducted hands-on workshops at Hack Space Con and Bsides Nova. Ryan has a Masters in Cybersecurity from GMU and the following Certifications: OSCP, OSEP, CRTO, GREM, GCFE, GCIH, CRTO

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 11:00-12:59 PDT

Title: Modifying Impacket for Better OpSec
When: Friday, Aug 9, 11:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

Operational security (OpSec) is a cornerstone in red teaming, necessitating continuous refinement of tools and techniques to avoid detection. This workshop is designed for new red team operators and individuals seeking to enhance their offensive capabilities. It focuses on customizing the Impacket toolset—a collection of Python classes for working with network protocols—to improve OpSec during engagements. Impacket tools such as wmiexec, smbexec, and secretsdump are staples in the toolkit of any red teamer due to their versatility and power in gaining access and extracting sensitive data from Windows environments. However, their detectability has increased as defensive measures have become more sophisticated. This session proposes modifications to these tools to reduce their footprint and evade modern security defenses. Participants will explore various customization strategies, including altering network signatures, timing attacks to evade detection, and integrating stealthier authentication methods. Practical exercises will guide attendees through the process of modifying the Impacket scripts, demonstrating how these changes can significantly enhance operational security in simulated environments.

SpeakerBio: Ryan O'Donnell, Senior Offensive Security Engineer at Microsoft

Ryan O'Donnell is an Offensive Security Engineer at Microsoft. Over the last 13+ years, Ryan has been performing Penetration Tests, Red Team assessments, and Incident Response investigations. Ryan has conducted hands-on workshops at Hack Space Con and Bsides Nova. Ryan has a Masters in Cybersecurity from GMU and the following Certifications: OSCP, OSEP, CRTO, GREM, GCFE, GCIH, CRTO

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 14:00-15:45 PDT

Title: Moriarty
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W307 - Map

Description:

Moriarty is a.NET tool designed to identify vulnerabilities for privilege escalation in Windows environments. Building upon Watson and Sherlock, Moriarty extends their capabilities by incorporating advanced scanning techniques for newer vulnerabilities and integrating additional checks. This tool supports a wide range of Windows versions, from Windows 10 to Windows 11 and Server versions 2016, 2019, and 2022. Moriarty differentiates itself by its ability to enumerate missing KBs and detect a variety of vulnerabilities linked to privilege escalation, offering suggestions for potential exploits. The tool's extensive database includes well-known vulnerabilities such as PrintNightmare (CVE-2021-1675), Log4Shell (CVE-2021-44228), and SMBGhost (CVE-2020-0796), among others.

Speakers: Anthony “Coin” Rose,Jake “Hubble” Krasnov

SpeakerBio: Anthony “Coin” Rose, Lead Security Researcher and Chief Operating Officer at BC Security

Anthony "Coin" Rose, CISSP, is a Lead Security Researcher and Chief Operating Officer at BC Security, where he specializes in adversary tactic emulation planning, Red and Blue Team operations, and embedded systems security. He has presented at numerous security conferences, including Black Hat, DEF CON, HackMiami, and RSA conferences. Anthony is the author of various offensive security tools, including Empire and Starkiller, which he actively develops and maintains. He is recognized for his work, revealing wide-spread vulnerabilities in Bluetooth devices and is the co-author of a cybersecurity blog at https://www.bc-security.org/blog/.

SpeakerBio: Jake “Hubble” Krasnov, Red Team Operations Lead and Chief Executive Officer at BC Security

Jake "Hubble" Krasnov is the Red Team Operations Lead and Chief Executive Officer of BC Security. He has spent the first half of his career as an Astronautical Engineer overseeing rocket modifications for the Air Force. He then moved into offensive security, running operational cyber testing for fighter aircraft and operating on a red team. Jake has presented at DEF CON, where he taught courses on offensive PowerShell and has been recognized by Microsoft for his discovery of a vulnerability in AMSI. Jake has authored numerous tools, including Invoke-PrintDemon and Invoke-ZeroLogon, and is the co-author of a cybersecurity blog at https://www.bc-security.org/blog/.

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 13:00-13:30 PDT

Title: MoWireless MoProblems: Modular Wireless Survey Systems and the Data Analytics That Love Them
When: Friday, Aug 9, 13:00 - 13:30 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Often there are times to collect #allTheWireless, but with that comes some planning, we've created a modular survey system and developed an Elastic-based analytic platform named PacketGlass to visualize and explore the terabytes of information collected over multiple surveys. Our system collects all data types supported by Kismet plus raw PCAP data, ingests the data, and displays tens of millions of devices in an easy to query and display manner. Using different parsing techniques, We plan to show how to build one of these survey platforms and discuss the methodology used to transform Elastic into a robust analytical platform.

Speakers: Geoff Horvath,Winson Tam

SpeakerBio: Geoff Horvath, Founder at Alsatian Consulting, LLC

Geoff Horvath is the founder of Alsatian Consulting, LLC. He has 13 years experience in the US Army as an intelligence officer specializing in signals intelligence. After leaving the military in 2021, he began researching and providing digital security assessments and recommendations. He currently advises private individuals, companies, and others in matters of privacy, security, and technology. He also once got kicked out of NSA Headquarters while looking for the gift shop.

SpeakerBio: Winson Tam

Winson Tam is a cybersecurity expert with over eight years of experience across government and private sectors. His work encompasses attacking, defending, and designing secure systems, notably for the US government, and a significant consulting career within the financial and industrial spaces. Tam's contributions in these areas have consistently resulted in tangible value and high customer satisfaction.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 12:00-13:45 PDT

Title: MPT - Pentest in Action
When: Saturday, Aug 10, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W307 - Map

Description:

In ever evolving software development world, security is also becoming fast paced. Hence, each product going through the pentest cycle has to be managed effectively and efficiently. Managing multiple pentests and testers is important. A single pane of glass view for managing pentests and testers is what the goal of this tool is.

SpeakerBio: Jyoti Raval, Senior Staff Product Security Leader at Baker Hughes

Jyoti Raval works as Senior Staff Product Security Leader at Baker Hughes. She is responsible for securing product end-to-end and involved in various phases of security life cycle. She is author of the Phishing Simulation Assessment and MPT tools, and has presented at Defcon, BlackHat, Nullcon, HITB, OWASP NZ and Infosec Girls. She also heads OWASP Pune chapter.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 20:00-01:59 PDT

Title: Music Set / Entertainment (Cyberpunk Bar Friday, ACK Stage)
When: Friday, Aug 9, 20:00 - 01:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

- 20:00 - 21:00 - Call the Cops
- 21:00 - 22:00 - DJ Habbs
- 22:00 - 23:00 - PankleDank
- 23:00 - 00:00 - Scotch & Bubbles
- 00:00 - 01:00- DJ St3rling
- 01:00 - 02:00 - Archwisp

Speakers: Scotch & Bubbles,PankleDank,DJ St3rling,DJ Habbs,Call the Cops,Archwisp

SpeakerBio: Scotch & Bubbles
No BIO available
SpeakerBio: PankleDank
No BIO available
SpeakerBio: DJ St3rling
No BIO available
SpeakerBio: DJ Habbs
No BIO available
SpeakerBio: Call the Cops
No BIO available
SpeakerBio: Archwisp
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 20:00-01:59 PDT

Title: Music Set / Entertainment (Cyberpunk Bar Saturday, ACK Stage)
When: Saturday, Aug 10, 20:00 - 01:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

- 20:00 - 21:00 - Kampf
- 21:00 - 22:00 - mattrix
- 22:00 - 23:00 - Dr. McGrew
- 23:00 - 00:00 - Magik Plan
- 00:00 - 01:00 - Syntax (DJ) + Luna (VJ)
- 01:00 - 02:00 - N8

Speakers: Wesley McGrew,Syntax (DJ) + Luna (VJ),N8,mattrix,Magik Plan,Kampf

SpeakerBio: Wesley McGrew, Senior Cybersecurity Fellow at MartinFederal

Dr. Wesley McGrew directs research, development, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented on topics of penetration testing and malware analysis at DEF CON and Black Hat USA and taught a self-designed course on reverse engineering to students at Mississippi State University, using real-world, high-profile malware samples. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems.

SpeakerBio: Syntax (DJ) + Luna (VJ)
No BIO available
SpeakerBio: N8
No BIO available
SpeakerBio: mattrix
No BIO available
SpeakerBio: Magik Plan
No BIO available
SpeakerBio: Kampf
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Thursday - 20:00-01:59 PDT

Title: Music Set / Entertainment (Cyberpunk Bar Thursday, ACK Stage)
When: Thursday, Aug 8, 20:00 - 01:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

- 20:00 - 21:00 - Stitcharoo
- 21:00 - 22:00 - Talk Sinn
- 22:00 - 23:00 - deaddoll
- 23:00 - 00:00 - CaptHz
- 00:00 - 01:00 - Relay
- 01:00 - 02:00 - Acid-T

Speakers: Talk Sinn,Stitcharoo,Relay,deaddoll,CaptHz,Acid-T

SpeakerBio: Talk Sinn
No BIO available
SpeakerBio: Stitcharoo
No BIO available
SpeakerBio: Relay
No BIO available
SpeakerBio: deaddoll
No BIO available
SpeakerBio: CaptHz
No BIO available
SpeakerBio: Acid-T
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 20:00-01:59 PDT

Title: Music Set / Entertainment (Pirate's Night For Me! Saturday, SYN Stage)
When: Saturday, Aug 10, 20:00 - 01:59 PDT
Where: LVCC West/Floor 2/W231-W233 - Map

Description:

- 20:00 - 21:00 - DJ Scythe
- 21:00 - 22:00 - Grindhaus Selektor
- 22:00 - 23:00 - Skittish and Bus
- 23:00 - 00:00 - Miss Jackalope
- 00:00 - 01:00 - O'Craven Celtic Pirate Band
- 01:00 - 01:15 - Costume Contest
- 01:15 - 02:00 - Ninjula

Speakers: Skittish and Bus,O'Craven Celtic Pirate Band,Ninjula,Miss Jackalope,Grindhaus Selektor,DJ Scythe,Costume Contest

SpeakerBio: Skittish and Bus
No BIO available
SpeakerBio: O'Craven Celtic Pirate Band
No BIO available
SpeakerBio: Ninjula
No BIO available
SpeakerBio: Miss Jackalope
No BIO available
SpeakerBio: Grindhaus Selektor
No BIO available
SpeakerBio: DJ Scythe
No BIO available
SpeakerBio: Costume Contest
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 20:00-01:59 PDT

Title: Music Set / Entertainment (Retro Sci-Fi Friday, SYN Stage)
When: Friday, Aug 9, 20:00 - 01:59 PDT
Where: LVCC West/Floor 2/W231-W233 - Map

Description:

- 20:00 - 20:45 - Icetre Normal
- 20:45 - 21:30 - Ohm-I & The NPC Collective
- 21:30 - 22:15 - Dual Core
- 22:15 - 23:00 - YTCracker
- 23:00 - 00:00 - MC Frontalot
- 00:00 - 00:15 - Costume Contest
- 00:15 - 01:15 - ZEE
- 01:15 - 02:00 - TRIODE

Speakers:ZEE,YTCracker,TRIODE,Ohm-I & The NPC Collective,MC Frontalot,Icetre Normal,Dual Core,Costume Contest

SpeakerBio: ZEE
No BIO available
SpeakerBio: YTCracker
No BIO available
SpeakerBio: TRIODE
No BIO available
SpeakerBio: Ohm-I & The NPC Collective
No BIO available
SpeakerBio: MC Frontalot
No BIO available
SpeakerBio: Icetre Normal
No BIO available
SpeakerBio: Dual Core
No BIO available
SpeakerBio: Costume Contest
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Thursday - 20:00-01:59 PDT

Title: Music Set / Entertainment (Thursday, SYN Stage)
When: Thursday, Aug 8, 20:00 - 01:59 PDT
Where: LVCC West/Floor 2/W231-W233 - Map

Description:

- 20:00 - 21:00 - Daemon Chadeau
- 21:00 - 22:00 - DotOrNot
- 22:00 - 23:00 - PatAttack
- 23:00 - 00:00 - DJ Vulp
- 00:00 - 01:00 - CTRL / rsm
- 01:00 - 02:00 - Grind613

Speakers: PatAttack,Grind613,DotOrNot,DJ Vulp,Daemon Chadeau,CTRL / rsm

SpeakerBio: PatAttack
No BIO available
SpeakerBio: Grind613
No BIO available
SpeakerBio: DotOrNot
No BIO available
SpeakerBio: DJ Vulp
No BIO available
SpeakerBio: Daemon Chadeau
No BIO available
SpeakerBio: CTRL / rsm
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 10:00-10:20 PDT

Title: Mutual authentication is optional
When: Saturday, Aug 10, 10:00 - 10:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Physical access control systems are often exploited in a number of ways. It could be weaknesses found within the credential itself, the antiquated communication protocol, the hardware itself, or the firmware it is running. But more often than not, it is a combination of factors that allow a variety of attacks from multiple dimensions. Some are extremely trivial and require little to no skill to perform, whereas some attacks require a bit more setup and knowledge of how the underlying technology works. We will go into detail on how these systems work, why verifying mutual authentication is important for physical access control systems and the exploits that can be accomplished, as well as ways to mitigate these exploits to make your facility more secure. This talk will include interactive demos involving official HID readers and hardware, proxmark3, and the flipper zero.

- link
- link
- link
- link
- link

SpeakerBio: Xavier Zhang

Xavier Zhang is a physical security consultant and security researcher working with RFID enabled technologies and physical access control systems. He is the author of numerous pieces of documentation in Iceman's proxmark3 repo such as the HID credential downgrade guide and an avid bug hunter in the proxmark3 community. Aside of physical security consulting, Xavier loves everything to do with DRM and reverse engineering how various forms of DRM are implemented in RFID tags. Currently Xavier is working on decoding the DRM used in a license violating closed source app based on the proxmark3 source, and all of the RFID tags it uses to help keep open source, open source.

Return to Index - Add to Google - ics Calendar file

AIV - Sunday - 11:00-11:30 PDT

Title: My Conversations with a GenAI-Powered Virtual Kidnapper
When: Sunday, Aug 11, 11:00 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

For the past few months, I've been seeing how far I can push several commercially available GenAI systems past their ethical boundaries. … hint: it's way too far.

In this talk, I'll demonstrate how I was able to turn LLMs into a powerful backend for realtime, interactive voice enabled cyber scams. I'll share my prompting strategy, social engineering tactics, the backend systems used, and show how each of these are working innocently in their own right, but enable massive possibilities for deception and harm when combined (in their current form). I'll also cover a few key insights gained from this research, including unexpected lessons from both successful and unsuccessful attempts.

Note: this session includes demos of a violent and profane chatbot. Please do not attend if that will be offensive to you.

SpeakerBio: Perry Carpenter, KnowBe4, Inc.
No BIO available

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 11:30-12:15 PDT

Title: My Smart Red Team Copilot
When: Saturday, Aug 10, 11:30 - 12:15 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Amid the Gen-AI revolution, notably through the rise of Large Language Models (LLMs), the cybersecurity landscape faces opportunities and challenges. These advanced AI models have successfully analyzed texts at unprecedented speeds, offering profound insights into vast data pools. However, this rapid technological growth has also paved the way for sophisticated Gen-AI-powered cyber threats that exploit these systems' adaptable, polymorphic nature, outpacing traditional defenses.

This presentation seeks to empower red teamers by unveiling the potential of open-source Gen-AI as a formidable ally in cybersecurity. Focusing on practical application, we will guide participants through constructing their own Gen-AI-based ""co-pilot,"" leveraging LLMs to enhance vulnerability identification and defense mechanisms.

Attendees will be introduced to the fundamentals of Gen-AI, including cost-effective strategies for fine-tuning LLMs using custom datasets drawn from pentest reports, bug bounties, and more. The discussion will extend to innovative, memory-efficient training methods such as LORA (Low-Rank Adaptation) and Quantized Low-Rank Adaptation (QLORA), making training an LLM on a modest single GPU setup feasible.

Designed for beginners with no prior AI experience, this talk aims to equip red teamers with powerful, open-source AI tools to accelerate vulnerability detection. By harnessing Gen-AI, cybersecurity professionals can stay one step ahead, identifying and mitigating potential threats at machine speed, ensuring they outpace adversaries in the ongoing cyber battle.

SpeakerBio: Gaspard Baye, AI Researcher & Ph.D. Candidate

Gaspard Baye, a PhD candidate in cyber-AI, brings over five years of industry experience, successfully leading teams to address over 100 critical challenges across 10 evaluations. His contributions include publishing six Cyber-AI algorithms, cited nearly 40 times in esteemed IEEE conferences and journals such as NeurIPS, PMLR, IEEE ISNCC, and IEEE/ACM MICRO'22. Recognized with a CVE for his cybersecurity work, Gaspard has fortified defenses for renowned firms like Nokia and Ford, earning places in multiple Hall of Fames.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 16:00-17:59 PDT

Title: Name the Noob
When: Friday, Aug 9, 16:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Name the Noob is a fun and interactive session where seasoned hackers create unique handles for new attendees. This activity helps newbies integrate into the hacking community and gives them a memorable start to their cybersecurity journey.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 15:00-17:59 PDT

Title: Name the Noob
When: Saturday, Aug 10, 15:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Name the Noob is a fun and interactive session where seasoned hackers create unique handles for new attendees. This activity helps newbies integrate into the hacking community and gives them a memorable start to their cybersecurity journey.

Return to Index - Add to Google - ics Calendar file

Title: Nano-Enigma: Uncovering the Secrets Within eFuse Memories
When: Saturday, Aug 10, 17:30 - 18:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

For years, eFuse-based memories were used to store sensitive information such as encryption keys, passwords, and other potentially confidential pieces of information. This practice was encouraged by several vendors who leverage such memory types for protecting the debugging interfaces using a password or for official way to store encryption keys for external flash memories.

However, with the advances in technology and threat actors' creativity, eFuse-based memories may take a hard hit on their confidentiality assurance as their physical properties could allow for a relatively easy extraction of the stored information.

In this talk we will walk you through the journey of revealing one such data storage from decapsulating the chip itself, delayering it using common household items all the way to using advanced tools such as Scanning Electron Microscope (SEM) to read value of an encryption key and thus break the confidentiality of the encrypted flash memory.

1. "Solving Chip Security's Weakest Link." Design & Reuse, April 1, 2023, link
2. Laurie, Adam. "Fun with Masked ROMs - Atmel MARC4." Adams Blog, rfidiot.org, 1 Jan. 2013, link
3. Hoover, William. "Looking Inside a 1970s PROM Chip That Could Change Computing." RightO, 19 July 2019, link
4. Chen, Nick. "The Benefits of Antifuse OTP." Semiconductor Engineering, 19 Dec. 2016, link

Speakers: Michal Grygarek,Martin Petran,Hayyan Ali

SpeakerBio: Michal Grygarek, Security Architect at Accenture

Michal has 20+ years of experience in the development of electronic systems and radio engineering. He specializes in cyber security of embedded systems, especially with relation to nanometer scale attack. His key expertise includes the methodology of decapsulation, delayering of silicon chips and their subsequent analysis using optical and electron microscopy.

SpeakerBio: Martin Petran, Embedded Systems Security Engineer at Accenture

Martin is an embedded systems security engineer with 9+ years of professional experience working at Accenture in Prague, Czech Republic. His main areas of focus are reverse engineering, fuzzing and exploit development. Throughout his career, he has created/contributed to several open-source projects and presented at security focused conferences.

SpeakerBio: Hayyan Ali, Security Delivery Senior Analyst at Accenture

Hayyan Ali brings over a decade of expertise in mobile communication, radio planning, and optimization to the forefront of cutting-edge technological advancements. Currently pursuing a Ph.D. at the Czech Technical University in Prague, Hayyan's research focuses on the integration of Machine Learning within mobile networks' radio interfaces. In addition to his academic pursuits, Hayyan serves as a Security Delivery Senior Analyst at Accenture, where he spearheads initiatives to fortify mobile communication infrastructures. Leveraging his extensive knowledge, he specializes in detecting vulnerabilities within radio interface protocols, conducting penetration testing on wireless interfaces in IoT devices, and deploying Machine Learning algorithms to automate pen testing processes.

Return to Index - Add to Google - ics Calendar file

XRV - Friday - 11:00-11:30 PDT

Title: National Labs Use of XR
When: Friday, Aug 9, 11:00 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

The DOE National Lab mission space includes exploring the use of disruptive technology to enable increasing efficiency and abilities of operations critical to national security, infrastructure, communication, and many other fields. The XR field has become a new area of active research and implementation at many national labs across the US, integrating with cutting edge hardware and software to enable users with increased capabilities. At the Pacific Northwest National Lab (PNNL), we have been using immersive XR platforms to enable a variety of government and external sponsors with novel approaches to their field. These include creating new 3D virtual twins to enable remote engagements as if remote users had access to one-of-a-kind lab equipment, creating simulation environments of hazardous environments or dangerous situations that can't be recreated in the real world, and outreach and communication projects to engage both sponsors and the public with critical information about current security threats. During this presentation I will touch on a few case studies of projects taken on at PNNL to make the best use of XR platforms, and where we see future development with this capability.

SpeakerBio: Martin Pratt, Lead, Immersive Computing Development Team at Pacific Northwest National Lab

Martin Pratt (AR/VR, software development, mobile & web app development, data visualization, subsurface geophysics): Software engineer. At the Pacific Northwest National Lab, Pratt leads the Immersive Computing development team, supporting efforts across a range of government agency mission spaces. He has worked on a number AR/VR projects including training simulations, data visualization, and educational games. He has developed software and subsurface 3D data visualizations that run on multiple platforms that include several public-facing applications.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 14:00-14:45 PDT

Title: Navigating Bureaucracy: Strategies for a Post-Military Career Encore
When: Saturday, Aug 10, 14:00 - 14:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:
SpeakerBio: Nia Luckey
No BIO available

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 13:00-13:59 PDT

Title: Navigating Microaggressions and Fostering Inclusive Communication with Peers and Leadership for Black Professionals

When: Saturday, Aug 10, 13:00 - 13:59 PDT

Where: LVCC West/Floor 3/W314-W316 - Map

Description:

This presentation dives into the critical role of emotional intelligence in navigating microaggressions and fostering inclusive communication dynamics for Black professionals in the cybersecurity field, particularly focusing on interactions with peers and leadership. It explores how developing emotional intelligence skills can equip Black cybersecurity professionals to effectively address and mitigate the impact of microaggressions while promoting respectful and inclusive communication exchanges within the team and with leadership.

SpeakerBio: Jessica Hoffman, DCISO & University Professor

No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 10:15-10:55 PDT

Title: Navigating the Cyber Security Labyrinth: Choose Your Own Security Adventure?
When: Saturday, Aug 10, 10:15 - 10:55 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Over the last 36 months, the cybersecurity landscape has evolved with unprecedented complexity, marked by ransomware, supply chain attacks, zero-days, remote work challenges, and more. Amid mass layoffs and pervasive mental burnout, organizations face daunting tasks in defending against escalating cyber threats. Layoffs exacerbate the skills gap, leaving teams stretched thin. Mental burnout hampers practitioners' abilities. In this talk, we'll explore the impacts of recent and chart a path forward for application security. As a lone AppSec professional, your choices will shape the future. Will you navigate through complexity or become lost in redundant complications?

SpeakerBio: punkcoder

James is a developer and security advocate who has lead developer security practices. He set the standards and procedures for how the engineering practices operate, and lead client engagement efforts with regard to cyber security. He also has lead company staff training to promote best practices with regard to security.

James has acted as a system and application architect, and evaluates application design as part of the security audits. In a past James was responsible for Architecture and developing solutions on multi-million implementation efforts. Key clients included the Eight Fortune 500 companies (Seven in the Fortune 100), as well as several well known non-profits and leaders in their industries. Vertices served included geospatial healthcare, transportation, financial services, retail, insurance, and energy.

In his free time James is involved with running BSides Boulder and AppSec Village @ DEFCON.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 10:00-11:45 PDT

Title: Nebula - 3 Years of Kicking *aaS and Taking Usernames
When: Friday, Aug 9, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W307 - Map

Description:

Cloud Penetration Testing has become a hot topic in the offensive community, as the cloud based infrastructures have been slowly taking the place on-prem ones used to have. This requires a tool to help with it. Nebula is a cloud Pentest Framework, which offers reconnaissance, enumeration, exploitation, post exploitation on AWS, Azure, DigitalOcean and above all opportunity to extend even more. It is built modulary for each provider and each attack, allowing for a diversity in attack surface. This coupled with the client-server architecture, allows for a collaborated team assessment of a hybrid cloud environment.

SpeakerBio: Bleon Proko

Bleon Proko is an info-sec passionate about Infrastructure Penetration Testing and Security, including Active Directory, Cloud (AWS, Azure, GCP, Digital Ocean), Hybrid Infrastructures, as well as Defense, Detection and Thread Hunting. He has presented in conferences like BlackHat and BSides on topics related to Cloud Penetration Testing and Security. His research include Nebula, a Cloud Penetration Testing Framework (https://github.com/gl4ssesbo1/Nebula) and other blogs, which you can also find on his blog (blog.pepperclipp.com). He is also the author of the upcoming book "Deep Dive into Clouded Waters: An overview in Digital Ocean's Pentest and Security" (https://leanpub.com/deep-dive-into-clouded-waters-an-overview-in-digitaloceans-pentest-and-security)

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Network-OS: Be The Cloud
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

The Network-OS workshop will take you into the mysterious world which underpins modern computing and allows people to talk across the globe. This of course being the network itself. In this workshop you will familiarize yourself with the command line of network devices. Step by step, you will configure devices to talk to each other, share information about the computers connected to them, and relay their network information and traffic between each other. No experience needed, know how to type and copy/paste.

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Network-OS: Be The Cloud
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

The Network-OS workshop will take you into the mysterious world which underpins modern computing and allows people to talk across the globe. This of course being the network itself. In this workshop you will familiarize yourself with the command line of network devices. Step by step, you will configure devices to talk to each other, share information about the computers connected to them, and relay their network information and traffic between each other. No experience needed, know how to type and copy/paste.

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Network-OS: Be The Cloud
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

The Network-OS workshop will take you into the mysterious world which underpins modern computing and allows people to talk across the globe. This of course being the network itself. In this workshop you will familiarize yourself with the command line of network devices. Step by step, you will configure devices to talk to each other, share information about the computers connected to them, and relay their network information and traffic between each other. No experience needed, know how to type and copy/paste.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 15:00-16:50 PDT

Title: New Skill Unlocked: C2 Infrastructure Automation
When: Friday, Aug 9, 15:00 - 16:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

Join us for an immersive workshop that will revolutionize your approach to Command-and-Control (C2) infrastructure deployments. Whether you're a seasoned Red Team operator or just starting your offensive security journey, this workshop is designed to equip you with the tools and knowledge to create scalable, operationally secure C2 infrastructure using the power of automation.

In this hands-on session, we'll demystify the process of deploying and configuring C2 components, such as frameworks, redirectors, and associated compute infrastructure.

You'll learn how to leverage infrastructure as code principles to create consistent, reliable, and secure C2 deployments, all while minimizing the risk of human error.

We'll dive deep into the best practices for designing and implementing C2 infrastructure automation, with a strong emphasis on operational security from the ground up.

Our instructor will guide you through real-world examples and provide you with a solid foundation for building your own secure C2 deployments.

Whether you're looking to enhance your Red Team capabilities or simply want to streamline your offensive security workflows, this workshop is perfect for you.

Join us and unlock the ability to spend less time on 'Sysadmin' tasks and more time focusing on what matters most – attacking and improving your organization's security posture!

No prior experience with C2 infrastructure automation is required.

Our instructor will guide you every step of the way, ensuring that you leave the workshop with the confidence and skills to create secure, automated C2 deployments.

Don't miss this opportunity to take your offensive security skills to the next level. Register now and unlock the power of secure C2 infrastructure automation!

Speakers: Josh Huff,Robert Pimentel

SpeakerBio: Josh Huff
No BIO available
SpeakerBio: Robert Pimentel
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 13:00-13:45 PDT

Title: No CTF? No Problem! Leveraging Alternate Reality Games to Develop OSINT and Cryptography Skills
When: Friday, Aug 9, 13:00 - 13:45 PDT
Where: LVCC West/Floor 2/W213-W214 - Map

Description:
SpeakerBio: John "2PAC" Smithberger
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: No Symbols When Reversing? No Problem: Bring Your Own
When: Friday, Aug 9, 11:00 - 11:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

We all know it all too well: that ominous feeling when opening an unknown file in your favorite analysis tool, only to be greeted with hundreds or thousands of unknown functions, none of which are matched by your existing function signatures, nor any of your helper scripts. This makes the analysis a painfully slow and tedious process. Additionally, it sometimes means that the required analysis time exceeds the available time, and another file is chosen to be reversed instead. Especially when dealing with malware, this is an undesired scenario, as it would create a blind spot from a blue team's perspective.

The goal of this talk is to share a tried and tested method on how to deal with thousands of unknown functions in a given file, significantly decreasing the time spent on the analysis. The example throughout the talk is the Golang based qBit family, but is applicable to any kind of binary. While this talk focuses on using Ghidra, given its free and open-source nature, it is equally possible with other industry standard tools. The focus will be on scripts, as well as the creation and usage of FunctionID and BSim databases. By combining these, you will be able to create your own symbols, and bring them anywhere you go, for any language of choice.

While the symbols are portable, an aggregation of them scales very well over any number of analysts. As such, this methodology works well for individual researchers, but when scaling it for a team of researchers, the outcome will be greater than the sum of its parts.

This talk will use (malicious) Golang binaries as examples and provide a large dataset of symbols for this language. The scripts, as well as FunctionID and BSim databases, mentioned in this talk will all be made publicly available at the time of this talk.

In no particular order:

- Automate .fidb generation with headless Ghidra: link
- Understanding static and dynamic compilation and linking: link
- How symbols work: link
- BSim answers from the Ghidra team: link
- Feeding Gophers to Ghidra (a blog I wrote for my employer about my research into Golang internals): link
- A blog I wrote summarising my Golang reversing journey for my employer: link
- The open-source scripts on GitHub: link
- A talk I gave about the Golang internals at HackInTheBox Amsterdam 2023: link
- Ghidra's FunctionID codebase: link
- Hex-Ray's IDA Pro's F.L.I.R.T. explained: link
- BSim's GhidraDoc explanation and tutorial: link

SpeakerBio: Max "Libra" Kersten

Max Kersten is a malware analyst, blogger, and speaker who aims to make malware analysis more approachable for those who are starting. In 2019, Max graduated cum laude with a bachelor's in IT & Cyber Security, during which Max also worked as an Android malware analyst. Currently, Max works as a malware analyst at Trellix, where he analyses APT malware and creates open-source tooling to aid such research. Over the past few years, Max spoke at international conferences, such as DEFCON, Black Hat (USA, EU, MEA, Asia), Botconf, Confidence-Conference, HackYeahPL, and HackFestCA. Additionally, he gave guest lectures and workshops for DEFCON, Botconf, several universities, and private entities.

AIxCC - Friday - 16:55-17:15 PDT

Title: No Time for Complacency: The Stakes of AI in Cybersecurity
When: Friday, Aug 9, 16:55 - 17:15 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Heather Adkins will pull from over 25 years of experience, including responding to major security incidents that impacted national security, to detail how the threat landscape has evolved into what it is today with the introduction of AI. She'll provide lessons learned by the industry in applying AI for security over the years, and explain how AI can be used in arming cyber defenders tasked with protecting the critical infrastructure we rely upon every day.

SpeakerBio: Heather Adkins, Vice President of Security Engineering at Google

Heather Adkins is a 22-year Google veteran and founding member of the Google Security Team. As head of Google's Office of Cybersecurity Resilience she leads the efforts to maintain the safety and security of Google's networks, systems and applications, and represents Google in government and industry forums globally. As deputy chair of CISA's Cyber Safety Review Board, she works to isolate the root causes of major security incidents impacting national security and make recommendations to policy-makers, standards bodies, and industry on improving the safety posture of modern computing. She is co-author of Building Secure and Reliable Systems (O'Reilly, 2020), is sought out to speak at high-profile conferences, and serves on the BlackHat review board. Heather advises numerous organizations on how to adopt modern defendable architectures, is a strategic advisor for a number of publicly-traded cybersecurity companies, and is a member of the steering committee for the IST Ransomware Taskforce. She is passionate about election security and was a senior advisor on the Defending Digital Democracy project at the Harvard Kennedy School's Belfer Center.

Heather Adkins, a seasoned cybersecurity expert with over two decades at Google, is a founding member of the Google Security Team. Currently heading Google's Office of Cybersecurity Resilience, she safeguards Google's vast digital infrastructure and represents the company in global technology and policy forums. Her influence extends to national security, as deputy chair of CISA's Cyber Safety Review Board, where she analyzes major security incidents and makes recommendations for policy-makers, standards bodies and industry. A recognized thought leader, Heather co-authored Building Secure and Reliable Systems (O'Reilly, 2020), is a sought-after speaker at major conferences, and serves on the BlackHat review board. She advises numerous organizations on modern security practices, including publicly-traded cybersecurity companies and as a member of the steering committee for the IST Ransomware Taskforce. A passionate advocate for election security, Heather served as a senior advisor on the Defending Digital Democracy project at Harvard's Kennedy School.

Return to Index - Add to Google - ics Calendar file

PLV - Friday - 15:00-16:45 PDT

Title: NSM-22 and the National Risk Management Plan: CISA Wants to Hear from You on How to Protect Our Nation's Critical Infrastructure
When: Friday, Aug 9, 15:00 - 16:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

On April 30th, the White House released National Security Memorandum-22 (NSM) on Critical Infrastructure Security and Resilience, which updates national policy on how the U.S. government protects and secures critical infrastructure from cyber and all-hazard threats. NSM-22 recognizes the changed risk landscape over the past decade and leverages the enhanced authorities of federal departments and agencies to implement a new risk management cycle that prioritizes collaborating with partners to identify and mitigate sector, cross-sector, and nationally significant risk. The culmination of this cycle is the creation of the National Infrastructure Risk Management Plan (National Plan)—thereby replacing the 2013 National Infrastructure Protection Plan—and will guide the Federal effort to mitigate cross-sector and national risks to critical infrastructure. As the National Coordinator for critical infrastructure security and resilience, CISA will develop this National Plan to be forward-looking and one that employs all available Federal tools, resources, and authorities to manage and reduce national-level risks, including those cascading across critical infrastructure sectors. In other words, the National Plan will be the federal government's comprehensive plan to mitigate and manage cross-sector risk. And that is why CISA is asking for you to help us and Sector Risk Management Agencies (SRMAs) over the course of the year as we develop this foundational document. During this session, two of the CISA leads when it comes to drafting this document will briefly walk through their approach, and then the rest of the session will be devoted to guided discussion and feedback.

Speakers: William Loomis,Michael Garcia

SpeakerBio: William Loomis, Cyber Policy Advisor for the Office of Strategy, Policy, and Plans at DHS Cyber Security and Infrastructure Security Agency

Will Loomis is a Cyber Policy Advisor for the Office of Strategy, Policy, and Plans at the Cybersecurity and Infrastructure Security Agency. He is also a nonresident fellow with the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab. Loomis previously served as an associate director with the Cyber Statecraft Initiative, where he led the program's work on critical infrastructure cybersecurity and software supply chain risk management. He was also formerly the chair of Young Professionals in Foreign Policy's Cybersecurity Policy & Technology Discussion Group and an organizer and Goon for Policy @ DEF CON.

SpeakerBio: Michael Garcia, Senior Policy Advisor for the Office of Strategy, Policy, and Plans at DHS Cyber Security and Infrastructure Security Agency

Michael Garcia is a senior policy advisor for the Office of Strategy, Policy, and Plans at the U.S. Cybersecurity and Infrastructure Security Agency (CISA) where he develops and supports interagency cybersecurity policies. Prior to joining CISA, Michael was a professional staff member for the U.S. Senate Homeland Security and Governmental Affairs Committee, where he worked on the Cyber Incident Reporting for the Critical Infrastructure Act of 2022 and other cybersecurity legislation. Before working for the Senate, Michael held several other cyber policy positions, including working at Third Way as a senior policy advisor for their Cyber Enforcement Initiative, serving as director for external engagement and outreach for the U.S. Cyberspace Solarium Commission, and advising governors' offices on cybersecurity policy issues at the National Governors Association. Michael was a 2020 fellow for New America and the Global Public Policy Institute's Transatlantic Digital Debate and a 2021 Next Gen National Security Fellow for the Center for New American Security. His work has been published and quoted by Politico, Lawfare, The Hill, Just Security, and the Council on Foreign Relations.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 13:30-14:15 PDT

Title: NTLM - The Last Ride
When: Saturday, Aug 10, 13:30 - 14:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

Microsoft is planning to kill off NTLM (New Technology Lan Manager) authentication in Windows 11 and above. Let's speedrun coercing hashes out of a few more things before it fades into obscurity over the next twenty five years or so.

There will be a deep dive on several new bugs we disclosed to Microsoft (including bypassing a fix to an existing CVE), some interesting and useful techniques, combining techniques from multiple bug classes resulting in some unexpected discoveries and some absolutely cooked bugs. We'll also uncover some defaults that simply shouldn't exist in sensible libraries or applications as well as some glaring gaps in some of the Microsoft NTLM related security controls.

1. link
2. link
3. link
4. link
5. Varonis Threat Labs discovered a new Outlook exploit and three new ways to access NTLM v2 hashed passwords. link

Speakers:Jim Rush,Tomais Williamson

SpeakerBio: Jim Rush

I'm a former software developer who has somehow ended up hacking things for a living, which is infinitely more fun as most of you know. I'm an active security researcher with several CVEs, including Blackboard, Moodle, Nuget, MS-Office and Kramer products.

SpeakerBio: Tomais Williamson

I'm an enthusiastic hacker who enjoys CTFs and have competed at an international level in the ICC CTF as well as being part of the CursedCTF 2024 winning team. I'm also an active security researcher with a bunch of CVEs and countless other bugs for a bunch of 'solved problems' in security.

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 10:00-10:30 PDT

Title: Obsidian: Forensics 101 Part 1
When: Saturday, Aug 10, 10:00 - 10:30 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:
An introduction to Digital Forensics: Part1

This is Part 1 of the Blue Team Village developed 101 tutorial series. This tutorial, which will be delivered in two parts, covers Digital Forensics basics. If you have ever been interested in Digital Forensics this series is a great place to start learning. The tutorials will cover the basics, and helps answer many of the questions regarding Digital Forensics and it's use in modern day digital investigations.

SpeakerBio: Sarthak Taneja
No BIO available

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 10:30-10:59 PDT

Title: Obsidian: Forensics 101 Part 2
When: Saturday, Aug 10, 10:30 - 10:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

An introduction to Digital Forensics: Part2

This is Part 2 of the Blue Team Village developed 101 tutorial series. This tutorial, which will be delivered in two parts, covers Digital Forensics basics. If you have ever been interested in Digital Forensics this series is a great place to start learning. The tutorials will cover the basics, and helps answer many of the questions regarding Digital Forensics and it's use in modern day digital investigations.

SpeakerBio: Sarthak Taneja

No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Octopus Game
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-A - Map

Description:

Get ready to dive into the excitement of the third annual Octopus Game at DEF CON! Octopus Game is your chance to connect with fellow attendees while exploring all the fun and fascinating aspects of DEF CON. Whether you're new to DEF CON, a beginner at code-breaking, or simply seeking a stress-free contest, this is the perfect opportunity for you. Test your skills in clue reading and code-breaking as you join in on the fun!

You and your fellow pirates will embark on an exhilarating journey, armed with clues that unveil the path to the lost treasure of a legendary pirate, now guarded by the mighty Kraken. These quests will guide you through the vibrant landscape of the Con, offering a glimpse into the myriad opportunities and experiences awaiting exploration. Designed to welcome newcomers to the hacking world, this contest fosters connections among attendees and contributors alike. Whether you choose to collaborate with a small group or brave the challenge solo, the decision is yours. Yet, amidst the excitement, remember that only one can emerge victorious. With challenges tailored for entry-level participants and a kid-friendly environment, come join us for a thrilling adventure into the depths of the Kraken's Conundrum.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Octopus Game
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-A - Map

Description:

Get ready to dive into the excitement of the third annual Octopus Game at DEF CON! Octopus Game is your chance to connect with fellow attendees while exploring all the fun and fascinating aspects of DEF CON. Whether you're new to DEF CON, a beginner at code-breaking, or simply seeking a stress-free contest, this is the perfect opportunity for you. Test your skills in clue reading and code-breaking as you join in on the fun!

You and your fellow pirates will embark on an exhilarating journey, armed with clues that unveil the path to the lost treasure of a legendary pirate, now guarded by the mighty Kraken. These quests will guide you through the vibrant landscape of the Con, offering a glimpse into the myriad opportunities and experiences awaiting exploration. Designed to welcome newcomers to the hacking world, this contest fosters connections among attendees and contributors alike. Whether you choose to collaborate with a small group or brave the challenge solo, the decision is yours. Yet, amidst the excitement, remember that only one can emerge victorious. With challenges tailored for entry-level participants and a kid-friendly environment, come join us for a thrilling adventure into the depths of the Kraken's Conundrum.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Octopus Game
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-06-A - Map

Description:

Get ready to dive into the excitement of the third annual Octopus Game at DEF CON! Octopus Game is your chance to connect with fellow attendees while exploring all the fun and fascinating aspects of DEF CON. Whether you're new to DEF CON, a beginner at code-breaking, or simply seeking a stress-free contest, this is the perfect opportunity for you. Test your skills in clue reading and code-breaking as you join in on the fun!

You and your fellow pirates will embark on an exhilarating journey, armed with clues that unveil the path to the lost treasure of a legendary pirate, now guarded by the mighty Kraken. These quests will guide you through the vibrant landscape of the Con, offering a glimpse into the myriad opportunities and experiences awaiting exploration. Designed to welcome newcomers to the hacking world, this contest fosters connections among attendees and contributors alike. Whether you choose to collaborate with a small group or brave the challenge solo, the decision is yours. Yet, amidst the excitement, remember that only one can emerge victorious. With challenges tailored for entry-level participants and a kid-friendly environment, come join us for a thrilling adventure into the depths of the Kraken's Conundrum.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 16:30-16:59 PDT

Title: Offensive Security Testing: Safeguarding the Final Frontier
When: Saturday, Aug 10, 16:30 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Every space mission is underpinned by critical software that spacecraft operators utilize to monitor and command their assets. The Mission Control System serves as the primary interface with a spacecraft, marking it as a crucial component of the ground segment. For decades, these systems were operated exclusively within the confines of mission control rooms, accessible only to a select group of individuals through a limited number of computer workstations. This paradigm has recently shifted, with numerous space organizations enabling their personnel to manage space assets remotely, including from the comfort of their homes. This increased accessibility has rendered space-related systems susceptible to the same security vulnerabilities that affect our daily-use software.

Despite the adoption of newer technology stacks in many mission control systems—either through upgrades or complete replacements—the consideration of security requirements has often been deferred to the final stages of development or overlooked entirely. This negligence presents a significant risk, exposing the space sector to potential exploitation by malicious entities. Like in other technology domains, merely expanding strategies to incorporate security measures, instituting security policies, and integrating new security requirements are positive but insufficient. Despite being developed and tested by extensive teams and presumably adhering to best practices, we have observed firsthand how contemporary mission control systems remain prone to elementary security flaws.

The most effective strategy to equip space systems with a robust defense against malicious actors involves integrating offensive security testing throughout their development lifecycle.

In this presentation, we share the results of the security research we have recently conducted on the more established, open-source Mission Control Systems: NASA OpenMCT and YaMCS. We present the details of the vulnerabilities we have discovered in those two systems, and their potential impact on a space mission when they are chained together into one exploit. We conclude by presenting with the audience the lessons learned from those security assessments.

SpeakerBio: Andrzej Olchawa

Andy Olchawa is an experienced Information Security Professional with over 15 years in the space industry, working as a Software Engineer and Technical Project Manager. For the past few years, he has focused on offensive security, specializing in vulnerability research, exploit development, and red team operations. He holds OSCP, OSWA, and OSWP certifications, and has been credited with several CVEs.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 13:00-13:45 PDT

Title: OH-MY-DC: Abusing OIDC all the way to your cloud
When: Saturday, Aug 10, 13:00 - 13:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

As DevOps and developers are slowly shifting away from storing long-lived static credentials to the more secure, still kinda-new, OIDC alternative - the underlying logic, mechanisms and implementations tend to feel like complicated magic and are mostly overlooked.

In this talk, we'll begin by recapping what OIDC is, who are the interacting entities when OIDC is used, and how OIDC is taking place to securely access one's cloud using CI/CD flows.

Once covered, we will be able to alternate our point-of-view between the entities in play and demonstrate potential vulnerabilities in various setups.

Starting with the user PoV, we will show what "under-configurations" look like, and continue by demonstrating how new OIDC configuration options can actually be misconfigurations that can result with a compromise.

We will then see another attack vector where leaking an OIDC token from a single repository in an organization can allow an attacker to abuse under-configurations and access private clouds.

After that, we will shift our PoV to be of the Identity Provider (IdP) so that we can look into what happens if an IdP is misconfigured, and disclose a real-world security vulnerability found in one of the most popular CI vendors that allowed us to access any of their customers' cloud environments.

I'll refer to this talk by the Tinder Security team link where they show how they could "claim" in the name of other identities due to under-configured WIFs.

SpeakerBio: Aviad Hahami, Palo Alto Networks

Security researcher and experienced software engineer with a great passion for algorithms (graph-theory specifically), security research (vulnerability research, bug bounties), chaos engineering (YES!), frontends, backends, web services, systems architecture, infras, clouds(making them rain), and more :)

Today, researching at Palo Alto Networks.

Oh yea I also DJ

Return to Index - Add to Google - ics Calendar file

DC - Friday - 12:00-12:45 PDT

Title: On Your Ocean's 11 Team, I'm the AI Guy (technically Girl)
When: Friday, Aug 9, 12:00 - 12:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

One of the best parts of DEF CON is the glitz and glam of Vegas, the gambling capital of the world. Many have explored hacking casinos (on and off stage). Unfortunately, it's just not like it is portrayed in the Oceans franchise.. in real life there's much less action, no George Clooney, and it's a lot harder to pull off a successful heist.

Fortunately I'm not your typical hacker, I'm an AI hacker. I use adversarial machine learning techniques to disrupt, deceive and disclose information from Artificial Intelligence systems.

I chose my target carefully: Canberra Casino. It's the best casino in my city.. It's also the only casino but that's not the point. The casino industry is at an interesting inflection point. Many large casinos have already adopted AI for surveillance and gameplay monitoring, smaller casinos are starting to make the transition, and there's only a couple of companies in the world that provide this software. It's ripe for exploitation.

In this talk I'm going to show you how I bypassed Casino Canberra's AI systems - facial recognition, surveillance systems and gameplay monitoring. AI Security is the new cyber security threat, and attacks on AI systems could have broad implications including misdiagnoses in medical imaging, navigation errors in autonomous vehicles.. and successful casino heists.

1. Standing Committee of the One Hundred Year Study of Artificial Intelligence. Gathering Strength,Gathering Storms: The One Hundred Year Study on Artificial Intelligence (AI100) 2021 Study Panel Report | One Hundred Year Study on Artificial Intelligence (AI100). Technical report, September 2021.
2. Eva A. M. van Dis, Johan Bollen, Willem Zuidema, Robert van Rooij, and Claudi L. Bockting. ChatGPT: five priorities for research. Nature, 614(7947):224–226, February 2023. Bandiera abtest: a Cg type: Comment Number: 7947 Publisher: Nature Publishing Group Subject term: Com-puter science, Research management, Publishing, Machine learning.
3. Mingfu Xue, Chengxiang Yuan, Heyi Wu, Yushu Zhang, and Weiqiang Liu. Machine Learn-ing Security: Threats, Countermeasures, and Evaluations. IEEE Access, 8:74720–74742, 2020.Conference Name: IEEE Access.
4. NSCAI. The National Security Commission on Artificial Intelligence.
5. Elisa Bertino, Murat Kantarcioglu, Cuneyt Gurcan Akcora, Sagar Samtani, Sudip Mittal, and Maanak Gupta. AI for Security and Security for AI. In Proceedings of the Eleventh ACM Confer-ence on Data and Application Security and Privacy, CODASPY '21, pages 333–334, New York, NY, USA, April 2021. Association for Computing Machinery.
6. Battista Biggio and Fabio Roli. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84:317–331, December 2018.
7. Ian Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and Harnessing Adversarial Examples. In International Conference on Learning Representations, 2015.
8. Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks, February 2014. arXiv:1312.6199 [cs].
9. Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pages 1528–1540, New York, NY, USA, October 2016. Association for Computing Machinery.
10. Tom Brown, Dandelion Mane, Aurko Roy, Martin Abadi, and Justin Gilmer. Adversarial Patch. 2017.
11. US Marines Defeat DARPA Robot by Hiding Under a Cardboard Box | Extremetech.
12. Walter David, Paolo Pappalepore, Alexandra Stefanova, and Brindusa Andreea Sarbu. AI-Powered Lethal Autonomous Weapon Systems in Defence Transformation. Impact and Chal-lenges. In Jan Mazal, Adriano Fagiolini, and Petr Vasik, editors, Modelling and Simulation for Autonomous Systems, Lecture Notes in Computer Science, pages 337–350, Cham, 2020. Springer International Publishing.

13. C Wise and J Plested. Developing Imperceptible Adversarial Patches to Camouflage Military Assets From Computer Vision Enabled Technologies, May 2022. arXiv:2202.08892 cs..
14. Anish Athalye, Nicholas Carlini, and David Wagner. Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples. In Proceedings of the 35th International Conference on Machine Learning, pages 274–283. PMLR, July 2018. ISSN: 2640-3498.
15. Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, and Dawn Song. Robust Physical-World Attacks on Deep Learning Visual Classification. In 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 1625–1634, Salt Lake City, UT, USA, June 2018. IEEE.
16. Ram Shankar Siva Kumar, Magnus Nystr †om, John Lambert, Andrew Marshall, Mario Goertzel, Andi Comissoneru, Matt Swann, and Sharon Xia. Adversarial Machine Learning-Industry Perspectives. In 2020 IEEE Security and Privacy Workshops (SPW), pages 69–75, May 2020.

SpeakerBio: Harriet Farlow, CEO at Mileva Security Labs

Harriet Farlow is the CEO of AI Security company Mileva Security Labs, a PhD Candidate in Machine Learning Security, and creative mind behind the YouTube channel HarrietHacks. She missed the boat on computer hacking so now she hacks AI and Machine Learning models instead. Her career has spanned consulting, academia, a start-up and Government, but don't judge her for that one. She also has a Bachelor in Physics and a Master in Cyber Security. She calls Australia home but has lived in the UK and the US. Her ultimate hack was in founding her own AI Security company but if Skynet takes over she will deny everything and pretend the AI stood for Artificial Insemination, like her Mum thinks it does. (Sorry Mum but I'm not really a Medical Doctor).

Return to Index - Add to Google - ics Calendar file

AIV - Friday - 15:00-15:59 PDT

Title: On Your Ocean's 11 Team, I'm the AI Guy (technically Girl)
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

One of the best parts of DEF CON is the glitz and glam of Vegas, the gambling capital of the world. Many have explored hacking casinos (on and off stage). Unfortunately, it's just not like it is portrayed in the Oceans franchise.. in real life there's much less action, no George Clooney, and it's a lot harder to pull off a heist than it seems.

Well fortunately I'm not your typical hacker, I'm an AI hacker. I use adversarial machine learning techniques to disrupt, deceive and disclose information from Artificial Intelligence systems. I chose my target carefully: Canberra Casino. It's the best casino in my city.. It's also the only casino but that's not the point.

The casino industry is at an interesting inflection point. Many large casinos have already adopted AI for surveillance and gameplay monitoring, smaller casinos are starting to make the transition, and there's only a couple of companies in the world that provide this software. It's ripe for exploitation.

In this talk I'm going to show you how I bypassed casino AI systems - facial recognition, surveillance systems and game monitoring. AI Security is the new cyber security threat, and attacks on AI systems could have broad implications including misdiagnoses in medical imaging, navigation errors in autonomous vehicles.. and successful casino heists.

SpeakerBio: Harriet Farlow, CEO at Mileva Security Labs

Harriet Farlow is the CEO of AI Security company Mileva Security Labs, a PhD Candidate in Machine Learning Security, and creative mind behind the YouTube channel HarrietHacks. She missed the boat on computer hacking so now she hacks AI and Machine Learning models instead. Her career has spanned consulting, academia, a start-up and Government, but don't judge her for that one. She also has a Bachelor in Physics and a Master in Cyber Security. She calls Australia home but has lived in the UK and the US. Her ultimate hack was in founding her own AI Security company but if Skynet takes over she will deny everything and pretend the AI stood for Artificial Insemination, like her Mum thinks it does. (Sorry Mum but I'm not really a Medical Doctor).

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 11:50-12:15 PDT

Title: One Click, Six Services: Abusing The Dangerous Multi-service Orchestration Pattern
When: Saturday, Aug 10, 11:50 - 12:15 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Cloud providers build their services a little like Jenga towers. They use their core services as the foundation of more popular customer-facing offerings. You may think you're just creating a GCP cloud function in an empty account. In reality, with one click, you're creating resources in six different services: a Cloud Build instance, a Storage Bucket, an Artifact Registry or a Container Registry, and possibly a Cloud Run instance and Eventarc triggers. The security of the entire stack is only as strong as the weakest link.

By looking at the entire stack, we can find privilege escalation techniques and even vulnerabilities that are hidden behind the stack. In my research, I was able to find a novel privilege escalation vulnerability and several privilege escalation techniques in GCP.

The talk will showcase a key concept, sometimes not discussed enough: cloud services are built on top of each other, and one click in the console can cause many things to happen behind the scenes. More services mean more risks and a larger attack surface.

The next part will dive deep into the vulnerable GCP cloud functions deployment flow. I will showcase the vulnerability I found in this flow, which enables an attacker to run code as the default Cloud Build service account by exploiting the deployment flow and the flawed trust between services resulting in a large fix and change in GCP IAM and Cloud Functions. This would grant an attacker high privileges to key services such as Storage, Artifact Registry, and Cloud Build.

However, this talk is about more than just a vulnerability. By understanding cross-service dependency, we can reveal a broad attack surface for many possible privilege escalation vectors between services. I will demo a simple tool I wrote to find the hidden APIs that are called by the CSP when performing an action.

By the end of this talk, the audience will learn the dangers of treating cloud services like a black box. The talk explains the hidden deployment flow behind one important stack, and provides the tools to uncover the risks of many more.

SpeakerBio: Liv Matan

Liv Matan (@terminatorLM) is a Senior Security Researcher at Tenable, where he specializes in application and web security. He previously worked as a Security Researcher at Ermetic and served in the Israeli Intelligence Corps as a Software Developer. As a bug bounty hunter, Liv has found several vulnerabilities in popular software platforms, such as Azure, Google Cloud, AWS, Facebook and Gitlab, was recognized by Microsoft as a Most Valuable Researcher, and has presented at conferences such as DEF CON Cloud Village and fwd:cloudsec. Liv studied computer science at the Weizmann Institute of Science, in Israel. In his free time, he boxes, lifts weights and plays Capture the Flag (CTF).

Return to Index - Add to Google - ics Calendar file

DC - Friday - 17:00-17:45 PDT

Title: One for all and all for WHAD: wireless shenanigans made easy !
When: Friday, Aug 9, 17:00 - 17:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

A lot of security research have recently focused on various wireless communication protocols, targeting smartphones, wireless mice and keyboards and even cars. In order to demonstrate these attacks, researchers developed dedicated tools that for most of them include some specialized firmware of their own but also rely on various unique custom host/device communication protocols. These tools work great but are strongly tied to some specific hardware that at some point will not be available anymore, or require hackers to buy more hardware to carry on to have fun with. Why not making these tools compatible with more hardware ? And why researchers always have to create their own host/device protocol when it comes to using a dedicated hardware ? Why not having one flexible protocol and related tools to rule them all ?

We will present in this talk WHAD, a framework that provides an extensible host/device communication protocol, dedicated protocol stacks and way more for hackers who love having fun with wireless protocols. WHAD makes interoperability possible between tools by allowing different hardware devices to be used if they provide the required capabilities, giving the opportunity to create advanced tools without having to care about the hardware and its firmware in most of the cases!

- [Atlas 2012] Atlas. SubGHz or Bust, 2012. Available at link.
- [Blu 2019] Bluetooth SIG. Bluetooth Core Specification, 2019.
- [Cauquil 2016] Damien Cauquil. BtleJuice: The Bluetooth Smart MiTM framework. In DEF CON, volume 24, 2016.
- [Cauquil 2017b] Damien Cauquil. Sniffing BTLE with the Micro:Bit. PoC or GTFO, vol. 17, pages 13–20, 2017.
- [Cauquil 2017c] Damien Cauquil. Weaponizing the BBC Micro:Bit. In DEF CON, volume 25, 2017. Available at link.
- [Cauquil 2018] Damien Cauquil. You'd better secure your BLE devices or we'll kick your butts ! In DEF CON, volume 26, 2018. Available at link.
- [Cauquil 2019] Damien Cauquil. Defeating Bluetooth Low Energy 5 PRNG for fun and jamming. In DEF CON, volume 27, 2019. Available at link.
- [Cayre 2019a] Romain Cayre, Vincent Nicomette, Guillaume Auriol, Eric Alata, Mohamed Kaâniche and Geraldine Marconato. Mirage: towards a Metasploit-like framework for IoT. In 2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE), Berlin, Germany, October 2019.
- [Cayre 2021b] Romain Cayre, Florent Galtier, Guillaume Auriol, Vincent Nicomette, Mohamed Kaâniche and Géraldine Marconato. InjectaBLE: Injecting malicious traffic into established Bluetooth Low Energy connections. In IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021), Taipei (virtual), Taiwan, June 2021.
- [Cayre 2021c] Romain Cayre, Florent Galtier, Guillaume Auriol, Vincent Nicomette, Mohamed Kaâniche and Géraldine Marconato. WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips. In IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021), Taipei (virtual), Taiwan, June 2021.
- [Cayre 2021d] Romain Cayre, Géraldine Marconato, Florent Galtier, Mohamed Kaâniche, Vincent Nicomette and Guillaume Auriol. Cross-protocol attacks: weaponizing a smartphone by diverting its Bluetooth controller. In 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, June 2021.
- [Cayre 2021e] Romain Cayre, Damien Cauquil and Aurélien Francillon. ESPwn32: hacking with ESP32 system-on-chips.In 17th IEEE Workshop on Offensive Technologies (WOOT 2023), co-located with IEEE S&P 2023, San Francisco, United States, May 2023.
- [Goodspeed 2011a] Travis Goodspeed. Promiscuity is the nRF24L01+'s Duty. Available at link, 2011.
- [IEE 2020] IEEE Standard for Low-Rate Wireless Networks. IEEE Std 802.15.4 2020 (Revision of IEEE Std 802.15.4-2015), pages 1–800, 2020.
- [Jasek 2016] Sławomir Jasek. Gattacking Bluetooth Smart Devices. In BlackHat USA, 2016. Available at link.
- [LOG 2019] LogiTacker GitHub Repository, 2019. Available at link
- [LoR 2017] LoRa Alliance, Inc. LoRaWan Specification, 2017.

- [Newlin 2016a] Marc Newlin. MouseJack : White Paper. In DEF CON, volume 24, 2016. Available at link.
- [Olawumi 2014] Olayemi Olawumi, Keijo Haataja, Mikko Asikainen, Niko Vidgren and Pekka Toivanen. Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned. In 2014 14th International Conference on Hybrid Intelligent Systems, pages 199–206, 2014.
- [Qasim Khan 2019] Sultan Qasim Khan. Sniffle: A sniffer for Bluetooth 5 (LE), 2019. Available at link.
- [Ryan 2013a] Mike Ryan. Bluetooth: With Low Energy Comes Low Security. In 7th USENIX Workshop on Offensive Technologies (WOOT 13), Washington, D.C., August 2013. USENIX Association.
- [Vidgren 2013a] N. Vidgren, K. Haataja, J. L. Patiño-Andres, J. J. Ramírez-Sanchis and P. Toivanen. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned. In 2013 46th Hawaii International Conference on System Sciences, pages 5132–5138, 2013.
- [Wright 2009] Joshua Wright. KillerBee: Practical ZigBee Exploitation Framework, 2009. Available at link.
- [Zillner 2015] T. Zillner. ZigBee Exploited: The good , the bad and the ugly. In BlackHat, 2015.

Speakers: Damien Cauquil,Romain Cayre

SpeakerBio: Damien Cauquil, Security Engineer at Quarkslab

Damien Cauquil is security engineer at Quarkslab, France. He loves electronics, embedded devices, wireless protocols and to hack all of these not especially in that order. He authored several Bluetooth Low Energy tools like Btlejuice and Btlejack, discovered a way to hack into an existing Bluetooth Low Energy connection that has later been improved by his co-speaker Romain Cayre, and other tools on a lot of different topics that tickle his mind but not always related to security or wireless protocols.

SpeakerBio: Romain Cayre, Assistant Professor, Software and System Security (S3) Group at EURECOM

Romain Cayre is assistant professor in Software and System Security (S3) group at EURECOM, France. He works on topics related to wireless security, IoT security and embedded systems security. He loves hacking embedded wireless stacks and playing with wireless protocols. In the past, he worked on several research projects related to wireless hacking, like WazaBee (a cross-protocol pivoting attack allowing to receive and transmit arbitrary 802.15.4 packets from a diverted BLE transceiver), InjectaBLE (an attack allowing to inject arbitrary packets into an ongoing Bluetooth Low Energy connection by leveraging a race condition in the Link Layer clock drift compensation mechanism), and OASIS (a defensive framework allowing to generate an embedded detection software and inject it into Bluetooth Low Energy controllers).

He is also the main developer of Mirage, an offensive framework for wireless communication protocols (and a draft to the new framework WHAD !)

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 12:10-12:30 PDT

Title: One Port to Serve Them All - Google GCP Cloud Shell Abuse
When: Friday, Aug 9, 12:10 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

The Cloud Shell feature from cloud service providers offers a convenient way to access resources within the cloud, significantly improving the user experience for both administrators and developers. However, even though the spawned instance has a short lifespan, granting excessive permissions could still pose security risks to users. This talk reveals an abuse methodology that leverages an unexpected, public-facing port in GCP Cloud Shell discovered during recon. Through manipulation in Linux Netfilter's NAT table, it serves various internally running services such as HTTP, SOCKS, and SSH within the Cloud Shell container to the public. This configuration could be exploited by adversaries to bypass the Google authentication needed in its Web Preview feature to leak data, to deliver malicious content, or to pivot attack traffic through the Google network.

SpeakerBio: Hubert Lin

Hubert Lin is an offensive security expert, specializing in remote vulnerability exploitation, honeypots, and penetration testing. He previously led the signature team for network threat defense and was a senior staff engineer on the Red Team at Trend Micro. In his roles, he assessed network intrusion prevention systems and conducted sanctioned red team exercises to enhance corporate security. Hubert holds certifications as a Red Hat Certified Engineer (RHCE) and an Offensive Security Certified Professional (OSCP). Currently, he works at Netskope as a Sr. Staff Researcher.

Return to Index - Add to Google - ics Calendar file

PYV - Saturday - 15:00-15:59 PDT

Title: Online Payments - Attack and Defense
When: Saturday, Aug 10, 15:00 - 15:59 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

"Learn the basics of how cards are used for payments online, and the risks associated. We'll explore a number of attacks used by malicious actors against online payment systems and the ways to mitigate them"

SpeakerBio: Vincent Sloan, GoFundMe

Vincent Sloan has been working in software and online payments for over 20 years and enjoys solving problems at the intersection for payments and security.

Return to Index - Add to Google - ics Calendar file

Title: Open Events for DCNextGen
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: Other / See Description

Description:

Open Events - All Days

AIxCC - Artificial Intelligence Cyber Challenge

Experience a dynamic model city with illuminated buildings and projections that bring to life the Semifinals of the AI Cyber Challenge (AIxCC) - a two-year competition to safeguard the software critical to modern life. You'll experience the thrill of the game events and the critical stakes of cybersecurity in an immersive setting that also offers an inspiring educational journey.

Social Engineering Village - SE Youth Challenge

The Social Engineering Community needs your help and it’s not exactly a big deal, but without your help, the entire universe is going to implode. Fortunately, some creative beings designed a failsafe just for this specific purpose, the Def Con Social Engineering Youth Challenge at DEF CON 32!

Adversary Village - Table top adventure

Tabletop adversary adventure!

Biohacking Village - Learn about bio-technology and biohacking!

Hands on medical device hacking and village tour

Ham Radio Vilage - Find the Fox, Decode a SSTV broadcast, get your Ham Radio License!

Fox Hunt!: Try to find the fox radio transmitter. SSTV: Send an SSTV broadcast and see it decoded by someone else Ham Radio Exam: Get your ham radio license at DEF CON!

Crypto Privacy Village - Gold Bug Puzzle

An invitation to a house party at the home of the Mysterious Marquise. What does it mean that it’s for those with “an adventurous spirit and enjoyment of puzzles”? And how can the doorknocker reveal anything? Find out in the Junior Cryptographer’s Corner of the CPV Gold Bug Puzzle.

Data Duplication Village - Multiple: HDD Teardown, Decryption Challenge, Error detection and correction

- **HDD Teardown**: Take apart and see how hard drives work.
- **Decryption Challenge**: Learn how file encryption / decryption works and solve a challenge.

- **Error Detection and Correction**: Use a simple binary code system, errors are introduced in the data string. Teaching basic parity checking or checksum algorithms to identify and correct the errors, demonstrating a fundamental data integrity concept.

Hardware Hacking Village - Open Soldering lessons

The folks at the Hardware Hacking Village can teach you soldering! Bring your soldering kits and learn this valuable hacker and life skill.

Friday, Saturday 13:00 - 16:00

Car Hacking Village Scavenger Hunt

The Car Hacking Village (CHV) put together a wonderland of fun for kids of all ages to explore. Stop by at our CHV Kids Booth during our hours of operation and dive into the rabbit hole of car hacking with our team. As you explore the CHV Village, you will not only learn about car hacking, but will also get to collect fun swag at every stop. Join us on this adventure through the car hacking wonderland and let your scavenger hunt begin.

Return to Index - Add to Google - ics Calendar file

Title: Open Events for DCNextGen
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: Other / See Description

Description:

Open Events - All Days

AIxCC - Artificial Intelligence Cyber Challenge

Experience a dynamic model city with illuminated buildings and projections that bring to life the Semifinals of the AI Cyber Challenge (AIxCC) - a two-year competition to safeguard the software critical to modern life. You'll experience the thrill of the game events and the critical stakes of cybersecurity in an immersive setting that also offers an inspiring educational journey.

Social Engineering Village - SE Youth Challenge

The Social Engineering Community needs your help and it’s not exactly a big deal, but without your help, the entire universe is going to implode. Fortunately, some creative beings designed a failsafe just for this specific purpose, the Def Con Social Engineering Youth Challenge at DEF CON 32!

Adversary Village - Table top adventure

Tabletop adversary adventure!

Biohacking Village - Learn about bio-technology and biohacking!

Hands on medical device hacking and village tour

Ham Radio Vilage - Find the Fox, Decode a SSTV broadcast, get your Ham Radio License!

Fox Hunt!: Try to find the fox radio transmitter. SSTV: Send an SSTV broadcast and see it decoded by someone else Ham Radio Exam: Get your ham radio license at DEF CON!

Crypto Privacy Village - Gold Bug Puzzle

An invitation to a house party at the home of the Mysterious Marquise. What does it mean that it’s for those with “an adventurous spirit and enjoyment of puzzles”? And how can the doorknocker reveal anything? Find out in the Junior Cryptographer’s Corner of the CPV Gold Bug Puzzle.

Data Duplication Village - Multiple: HDD Teardown, Decryption Challenge, Error detection and correction

- **HDD Teardown**: Take apart and see how hard drives work.
- **Decryption Challenge**: Learn how file encryption / decryption works and solve a challenge.

- **Error Detection and Correction**: Use a simple binary code system, errors are introduced in the data string. Teaching basic parity checking or checksum algorithms to identify and correct the errors, demonstrating a fundamental data integrity concept.

Hardware Hacking Village - Open Soldering lessons

The folks at the Hardware Hacking Village can teach you soldering! Bring your soldering kits and learn this valuable hacker and life skill.

Friday, Saturday 13:00 - 16:00

Car Hacking Village Scavenger Hunt

The Car Hacking Village (CHV) put together a wonderland of fun for kids of all ages to explore. Stop by at our CHV Kids Booth during our hours of operation and dive into the rabbit hole of car hacking with our team. As you explore the CHV Village, you will not only learn about car hacking, but will also get to collect fun swag at every stop. Join us on this adventure through the car hacking wonderland and let your scavenger hunt begin.

Return to Index - Add to Google - ics Calendar file

Title: Open Events for DCNextGen
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: Other / See Description

Description:

Open Events - All Days

AIxCC - Artificial Intelligence Cyber Challenge

Experience a dynamic model city with illuminated buildings and projections that bring to life the Semifinals of the AI Cyber Challenge (AIxCC) - a two-year competition to safeguard the software critical to modern life. You'll experience the thrill of the game events and the critical stakes of cybersecurity in an immersive setting that also offers an inspiring educational journey.

Social Engineering Village - SE Youth Challenge

The Social Engineering Community needs your help and it’s not exactly a big deal, but without your help, the entire universe is going to implode. Fortunately, some creative beings designed a failsafe just for this specific purpose, the Def Con Social Engineering Youth Challenge at DEF CON 32!

Adversary Village - Table top adventure

Tabletop adversary adventure!

Biohacking Village - Learn about bio-technology and biohacking!

Hands on medical device hacking and village tour

Ham Radio Vilage - Find the Fox, Decode a SSTV broadcast, get your Ham Radio License!

Fox Hunt!: Try to find the fox radio transmitter. SSTV: Send an SSTV broadcast and see it decoded by someone else Ham Radio Exam: Get your ham radio license at DEF CON!

Crypto Privacy Village - Gold Bug Puzzle

An invitation to a house party at the home of the Mysterious Marquise. What does it mean that it’s for those with “an adventurous spirit and enjoyment of puzzles”? And how can the doorknocker reveal anything? Find out in the Junior Cryptographer’s Corner of the CPV Gold Bug Puzzle.

Data Duplication Village - Multiple: HDD Teardown, Decryption Challenge, Error detection and correction

- **HDD Teardown**: Take apart and see how hard drives work.
- **Decryption Challenge**: Learn how file encryption / decryption works and solve a challenge.

- **Error Detection and Correction**: Use a simple binary code system, errors are introduced in the data string. Teaching basic parity checking or checksum algorithms to identify and correct the errors, demonstrating a fundamental data integrity concept.

Hardware Hacking Village - Open Soldering lessons

The folks at the Hardware Hacking Village can teach you soldering! Bring your soldering kits and learn this valuable hacker and life skill.

Friday, Saturday 13:00 - 16:00

Car Hacking Village Scavenger Hunt

The Car Hacking Village (CHV) put together a wonderland of fun for kids of all ages to explore. Stop by at our CHV Kids Booth during our hours of operation and dive into the rabbit hole of car hacking with our team. As you explore the CHV Village, you will not only learn about car hacking, but will also get to collect fun swag at every stop. Join us on this adventure through the car hacking wonderland and let your scavenger hunt begin.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 12:00-13:45 PDT

Title: Open Hardware Design for BusKill Cord
When: Saturday, Aug 10, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W303 - Map

Description:

An open hardware design for BusKill cables that uses 3D printing and easily sourceable components. BusKill cables are hardware Dead Man's Switches that use USB events to trigger a laptop to lock, shutdown, or self-destruct when the laptop is physically separated from the operator.

SpeakerBio: Melanie Allen

Melanie Allen is a 3D-printing enthusiast and volunteer hardware developer with the BusKill project.

Return to Index - Add to Google - ics Calendar file

Title: Open sesame - or how vulnerable is your stuff in electronic lockers
When: Sunday, Aug 11, 11:30 - 12:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Physical security is often overlooked in many organizational threat models. An increasing amount of physical security devices with smart components are being introduced to the market with widespread adoption. This creates an enticing attack surface for physical red teams.

Lockers and cabinets equipped with electronic smart locks can be found in many places such as offices, factories, hospitals, labs, and gyms. With remote and hybrid work increasing in popularity, shared use office setups becoming the default. Co-working spaces in offices are now commonplace with lockers being installed for employee device storage. People generally trust that their belongings will be secure in these lockers and entrust the locks with sensitive information, like their personal PIN.

Is there a more stealthy way to get into lockers that don't involve using a crowbar?

In this talk we will analyze the vulnerabilities affecting locks manufactured by the "global leader in keyless lock solutions," Digilock and Schulte-Schlagbaum AG (SAG). Both companies have been in the physical security industry for many decades. What went wrong in the development of these devices and how can these vulnerabilities be fixed? We will also discuss several other vendors operating in this space and compare findings.

We will demonstrate practical physical and side-channel attacks targeting locks that accept a standard PIN and RFID. Learn why it is poor practice to reuse the same secret PIN for lockers and safes and devices such as mobile phones and laptops (especially if they are stored inside the lockers).

Speakers:Dennis Giese,Braelynn

SpeakerBio: Dennis Giese

Dennis Giese is a researcher with the focus on the security and privacy of IoT devices. While being interested in physical security and lockpicking, he enjoys applied research and reverse engineering malware and all kinds of devices. His most known projects are the documentation and hacking of various vacuum robots. He calls himself a "robot collector" and his current vacuum robot army consists of over 60 different models from various vendors. He talked about his research at the Chaos Communication Congress, REcon BRX, NULLCON, and DEFCON.

SpeakerBio: Braelynn, Security Consultant at Leviathan Security Group

Braelynn is a security consultant at Leviathan Security Group where she conducts security assessments of products for startups, Fortune 500 companies, and everything in between. She enjoys partaking in CTFs and researching the security anything that piques her curiosity. She has previously presented this research at conferences such as Chaos Communication Congress.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 13:30-14:30 PDT

Title: Open Source Drone Hacking Simulator
When: Saturday, Aug 10, 13:30 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

Drone hacking tends to be expensive and sometimes unsafe, but not if you use a simulator!. We have developed a drone hacking simulator called the Damn Vulnerable Drone (https://github.com/nicholasaleks/Damn-Vulnerable-Drone).

The Damn Vulnerable Drone is a virtually simulated environment designed for offensive security professionals to safely learn and practice drone hacking techniques. It simulates real-world ArduPilot & MAVLink drone architectures and vulnerabilities, offering hands-on experience in exploiting drone systems.

Speakers: Nick Aleks,Rudy Mendoza

SpeakerBio: Nick Aleks
No BIO available
SpeakerBio: Rudy Mendoza

Rudy Mendoza is a highly skilled Penetration Tester at Dark Wolf Solutions with seven years of extensive experience in the field of Cyber Security. Renowned for his expertise, Rudy has achieved notable acclaim, including winning the prestigious Black Badge with his team at the DefCon IoT village CTF in 2022.

Rudy has played a major role in paving the way for drone penetration testing, as one of the main pentesters for the BlueUAS program, he has been instrumental in enhancing the security and reliability of these critical systems. Rudy created "The Drone Wolf Playbook," which has been widely regarded as an essential resource in drone security. His background as an Air Force Veteran further enhances his depth of knowledge and tactical proficiency in cybersecurity.

Rudy's diverse experiences and accolades make him a respected figure in the cybersecurity community, and he brings a wealth of knowledge and insight to every conference and workshop he participates in.

Return to Index - Add to Google - ics Calendar file

PLV - Friday - 15:15-15:59 PDT

Title: Open Source Hacker Vs. Government Lawyer: Clashing Views on Fixing Tech in the DoD
When: Friday, Aug 9, 15:15 - 15:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

“What do you mean I can’t bring my car keys into this building?”

“No internet?? But how do I download things from GitHub?”

Join a recovering government attorney and an open-source hacker for a fiery debate that dives into the world of DoD cybersecurity inefficiencies. Rebecca, a former DoD lawyer, pairs her intricate understanding of perplexing government policies with Eddie’s fresh, critical (and dare we say naive?) insights from the private sector. This session will explore the frustrating “how” behind the government’s “why,” from slow booting government laptops to the realities of “military-grade technology.” Together, they will challenge the status quo, proposing innovative, open-source inspired solutions to streamline and secure DoD operations. Expect a dynamic exchange filled with real-world frustrations, enlightening explanations, and a hacker’s touch on how to fix what’s broken.

Speakers: Eddie Zaneski,Rebecca Lively

SpeakerBio: Eddie Zaneski, Open Source Tech Lead at Defense Unicorns

Eddie Zaneski lives in Denver, CO with his wife and dog. He loves open source and helps lead the Kubernetes project. His day job is building OSS for the US Government. When not hacking on random things you'll most likely find him climbing rocks somewhere.

SpeakerBio: Rebecca Lively, Polymath at Defense Unicorns

Rebecca K. Lively began her career as an attorney focusing on legal and policy issues relating to software development, acquisition, intellectual property, and cyberspace operations. In 2020 she went all-in on software development, co-founding Shadow’s Edge Software, Air Force Cyber’s Software Factory. As a product strategist at Defense Unicorns, Rebecca leverages her diverse background to build solutions to streamline software delivery and cybersecurity in highly regulated environments. Rebecca lives in Texas with her spouse and a handful of children. She does not consider herself responsible enough for pet ownership.

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 10:00-10:10 PDT

Title: Opening Note
When: Friday, Aug 9, 10:00 - 10:10 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

AIV - Friday - 10:00-10:30 PDT

Title: Opening Remarks
When: Friday, Aug 9, 10:00 - 10:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

Opening remarks for events at AIV at DEFCON 32

Speakers: Sven Cattell,Lauren Putvin,Ravin Kumar

SpeakerBio: Sven Cattell, Founder at AI Village
No BIO available
SpeakerBio: Lauren Putvin, AIV Steering Committee
No BIO available
SpeakerBio: Ravin Kumar, AIV Steering Committee
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Friday - 14:00-14:45 PDT

Title: Optical Espionage: Using Lasers to Hear Keystrokes Through Glass Windows
When: Friday, Aug 9, 14:00 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

Sashay away from this talk with the knowledge to perform state-of-the-art espionage, no technical background required.

In the realm of privilege escalation and data exfiltration, the physical world quietly screams secrets. We'll demystify the fascinating physics behind signals and how various forms of energy--infrared, visible, and ultraviolet light, radio, ultrasound, audible sound, mechanical vibration, and temperature--can be interpreted as waves that unintentionally leak information, even in air-gapped (non-networked) systems. We'll observe how air is in fact not an effective gap or barrier as radio, light, sound, and vibration excitedly travel through it. We'll explore how all electrical signals radiate electromagnetism (light or radio) that can be intercepted and how we can reverse this process, producing electromagnetism to inject desired electrical signals into our target.

We'll delve into historical and seminal side-channel/TEMPEST attacks from our friends at the NSA, KGB, and past DEF CON pioneers. You'll learn about the essential electrical and optical components combined for cutting-edge eavesdropping, including what our target is typing from a distance.

While others believe they're obtaining noise, we will extract signal, and you'll leave this talk hearing the world in a new light.

- [1985] Electromagnetic radiation from video display units - Wim van Eck
- Bunnie link
- DEFCON 17: Sniff Keystrokes With Lasers/Voltmeters - Andrea Barisani, Daniele Bianco
- DEF CON 23 - Colin Flynn - Dont Whisper my Chips: Sidechannel and Glitching for Fun and Profit
- DEF CON 24 - Marc Newlin - MouseJack: Injecting Keystrokes into Wireless Mice
- DEF CON 25 - Matt Wixey - See no evil, hear no evil: Hacking invisibly & silently with light & sound
- DEF CON 31 - Video Based Cryptanalysis Extracting Keys from Power LEDs - Ben Nassi, Ofek Vayner
- Georgi Gerganov - kbd-audio link
- Lest We Remember: Cold Boot Attacks on Encryption Keys - Halderman et al link
- RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis - Daniel Genkin, Adi Shamir, Eran Tromer link

SpeakerBio: samy kamkar

Samy Kamkar is a security researcher, sometimes known for creating The MySpace Worm, the fastest spreading (non-biological) virus of all time. As a teenager, this led to a raid by the Secret Service and a court-ordered ban from computers, the Internet, and MySpace. After years of virtuous, upstanding behavior and a legal technological reinstatement, he now attempts to develop and illustrate terrifying vulnerabilities with playfulness, where his exploits have been branded:

“Controversial” -The Wall Street Journal

“Horrific” -The New York Times

“Now I want to fill my USB ports up with cement” -Gizmodo

Samy's open source software, hardware, and research highlight insecurities and privacy implications in everyday technologies. From NAT Slipstreaming and Evercookies, which bypass firewalls by simply visiting a web page and produce virtually immutable respawning cookies, to RollJam and SkyJack, a cryptography-agnostic radio-based car exploitation device and drones that wirelessly hijack and autonomously control swarms of other drones within wireless distance.

His work has been cited by the NSA, triggered hearings on Capitol Hill, and is the basis for security advancements across nearly all major web browsers, smartphones, and vehicles.

Return to Index - Add to Google - ics Calendar file

Title: OSINT at Clemson: Unmasking John Mark Dougan's Disinformation Empire
When: Friday, Aug 9, 17:45 - 18:15 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Clemson University's Media Forensics Center spearheaded an investigation into the extensive disinformation network orchestrated by John Mark Dougan, an alleged corrupt Sheriff's Deputy now residing in Russia. This presentation will focus on Clemson's employment of OSINT techniques, emphasizing our thorough examination of digital forensic artifacts and metadata analysis.

Through advanced OSINT techniques, our team analyzed server logs, domain registrations, and internet protocol (IP) addresses, unraveling a sophisticated web of over 160 disinformation websites designed to mimic legitimate news outlets. By dissecting these digital breadcrumbs, we traced the network's infrastructure and operational tactics, uncovering the strategies Dougan employed to disseminate false narratives. During the process we discovered how narratives were laundered, and LLMs were utilized to create inflammatory content.

The session will provide a detailed look at the methods used to collect and interpret metadata and artifacts, which revealed the hidden connections between the fake sites and Dougan's operations. We will discuss how our forensic analysis uncovered patterns of digital behavior, allowing us to attribute the network's activities to Dougan and understand the broader implications for more transparent public discourse.

Join us as we share the intricacies of our forensic process, demonstrating how Clemson's expertise in media forensics and metadata analysis played a critical role in exposing a key player in Russia's disinformation efforts. This talk will equip attendees with a deeper appreciation of the vital role OSINT plays in modern intelligence operations and the ongoing battle against digital deception.

SpeakerBio: Steven Sheffield
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 11:00-11:50 PDT

Title: OSINT for Hackers
When: Saturday, Aug 10, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Ascension - Map

Description:

In this Workshop, attendees will learn some of the most impactful techniques and tools to increase the value of OSINT to their organizations. A guided learning experience, instructors will immerse attendees in hands-on exercises.

Speakers: Lee McWhorter,Sandra Stibbards

SpeakerBio: Lee McWhorter
No BIO available
SpeakerBio: Sandra Stibbards
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: OT Incident response and Threat Hunting
When: Friday, Aug 9, 15:30 - 15:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

In the rapidly evolving landscape of cybersecurity, operational technology (OT) systems are increasingly becoming prime targets for cyber attacks. As a result, the adoption of effective incident response plans and threat hunting strategies has become essential for organizations to protect their critical OT infrastructure. This presentation will discuss the importance of OT incident response and threat hunting, as well as the challenges faced by the OT industry in implementing these cybersecurity measures.

One of the key challenges in the OT industry is the complexity and interconnectivity of OT systems, which often consist of legacy equipment and proprietary protocols that can be difficult to monitor and secure. Additionally, the lack of visibility into OT networks and the limited availability of skilled cybersecurity professionals with OT expertise pose significant obstacles in detecting and responding to cyber threats in a timely manner. Moreover, the convergence of IT and OT environments further complicates incident response efforts, as organizations must navigate the unique requirements and operational constraints of both domains.

Despite these challenges, we will provide you with tools and frameworks to help overcome them by implementing a proactive approach to incident response and threat hunting in OT environments. This includes conducting architecture, passive, and active defense mechanisms and strategies in the OT environments. By addressing these challenges head-on and fostering collaboration between IT and OT teams, organizations can enhance their cybersecurity posture and effectively defend against cyber threats targeting their OT systems.

Speakers: Adam Robbie,Bradley Nash

SpeakerBio: Adam Robbie, Head of OT Security Research at Palo Alto Networks

Adam is the Head of OT Security Research at Palo Alto Networks since 2022 with over 10 years of experience in both OT and IT industries. Publisher and author with SANS, IEEE, and other journals and conferences. His ambition is about contributing to secure our critical infrastructure, search for recent vulnerabilities, develop best practices and lead new initiatives. Adam has a Bachelor and Master of Science in Electrical Engineering. Additionally, he obtained advanced certifications including the Global Industrial Cyber Security Professional (GICSP) and GIAC Response and Industrial Defense (GRID) certifications.

In addition to his technical expertise, He has a strong background in leadership and education. As an Adjunct Professor, he has been teaching cybersecurity bootcamp at The George Washington University, University of Michigan, University of Wisconsin, and other universities. Through these roles, he has successfully mentored and guided students, encouraging them to excel in the field of cybersecurity. Additionally he served as an advisor for developing cybersecurity curriculum across different universities.

During his tenure as a Senior Cyber Security Consultant at Deloitte, he gained extensive experience in performing ICS/IoT penetration testing, threat hunting, risk assessment, and vulnerability research. Furthermore, he has actively contributed to enhancing detection systems through advanced research and creation of security use cases.

SpeakerBio: Bradley Nash, IIT Perimeter Security Supervisor at ExxonMobil Corporation

Brad is a seasoned IT professional with diverse expertise in network communications, cybersecurity, and project management. Brad has accumulated over a decade of experience in roles spanning IT operations, security, and analysis of both hardware and software. Majority of Brad’s experience comes from being in the field as he has moved around the country learning each area’s unique challenges. That experience helps Brad interface with the business needs for projects, work prioritization within

the team, and system assessment and hardening in his role of IIT Perimeter Security Supervisor. Brad holds an Associates of Science in System Administration and Bachelor of Science in Network Communications and Management from DeVry University. Brad's dedication to efficiency and problem-solving has made him a valuable asset in optimizing IT operations and ensuring robust cybersecurity measures. With a strong foundation in network communications, Brad's impact on IT organizations is characterized by his commitment to excellence and technical proficiency.

Return to Index - Add to Google - ics Calendar file

Title: Outlook Unleashing RCE Chaos: CVE-2024-30103 & CVE-2024-38021
When: Friday, Aug 9, 16:00 - 16:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Did you ever receive an empty email and immediately think it might be a reconnaissance attack? What if opening such an email in your Outlook client could trigger remote code execution through an invisible form? Yes, all forms are COM objects, and CVE-2024-21378 has flung open the gates to Outlook RCE chaos.

In our session, "Outlook Unleashing RCE Chaos: CVE-2024-30103" we'll dive into how this seemingly innocuous vulnerability can lead to mayhem. This vulnerability paved the way for us to discover a series of new remote code execution vulnerabilities in Outlook, including CVE-2024-30103. But we're not stopping there.

Additionally, we'll uncover other vulnerabilities that can cause NTLM leaks from your domain-joined devices.

So, how did we get here? Join us as we construct an evolution timeline of this attack surface. From the origins of these exploits to their current incarnations, we'll cover it all. And because we believe in building a safer digital world, we'll conclude with specific, actionable recommendations on how to minimize these threats.

1. link
2. link
3. link
4. link
5. link
6. link

Speakers: Michael Gorelik ,Arnold Osipov

SpeakerBio: Michael Gorelik , Founder at Morphisec

Michael has amassed over twenty years of experience in the cybersecurity industry, with a decade at Morphisec where he pioneered Moving Target Defense within Endpoint Security. Prior to founding Morphisec, he collaborated on numerous security projects with Deutsche Telekom and Ben-Gurion University laboratories. His expertise spans roles as a reverser, malware researcher, penetration tester, and vulnerability researcher. Michael holds more than seven patents and a Master of Science degree in Computer Science from Ben-Gurion University, Israel. He has worked with the FBI on several significant cybersecurity cases and identified critical privilege escalation exploits in various endpoint security vendors. Michael is a seasoned speaker at industry conferences and led his team to uncover one of the largest supply chain attacks, the CCleaner incident.

SpeakerBio: Arnold Osipov, Distinguished Malware Researcher at Morphisec

Arnold is a distinguished malware researcher at Morphisec, renowned for discovering new categories of malware, including the Jupyter and Chaos info stealers among others. His groundbreaking work has significantly advanced understanding and mitigation of emerging malware threats. Arnold has presented his findings at various BSides events throughout Europe, establishing himself as a knowledgeable and engaging speaker. His research continues to push the boundaries of cybersecurity, enhancing both Morphisec's capabilities and the broader security landscape.

RCV - Saturday - 12:00-13:59 PDT

Title: OWASP Amass Expanding Data Horizons: Amassing More Than Subdomains
When: Saturday, Aug 10, 12:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Join us at Recon Village for an in-depth workshop on the OWASP Amass Project, a powerful open-source tool used for network mapping, attack surface analysis, and asset discovery. This workshop will delve into the exciting advancements in data collection capabilities within Amass, demonstrating how these enhancements have taken the project from a humble subdomain enumeration tool to an OSINT collection system. Participants will gain hands-on experience with new features, learn best practices for leveraging Amass, and explore the broader dataset of findings and associated assets. Whether you are a seasoned security professional or new to network reconnaissance, this session will provide valuable insights and practical skills to elevate your reconnaissance game.

Workshop Outline

Introduction (15 minutes) - Welcome and speaker introductions - Overview of OWASP Amass - Brief history and evolution - Core functionalities and typical use cases - Workshop objectives and agenda

Understanding Amass's Data Collection Capabilities (15 minutes) - Current data sources utilized by Amass - Public data sources - OSINT (Open Source Intelligence) integration - Third-party APIs - Introduction to new data collection features - Enhanced API integrations - Proprietary data sources

Hands-On with New Data Collection Features (30 minutes) - Setting up Amass for expanded data collection - Installation and configuration - API key management and integration - Practical demonstration - Running Amass with new data sources - Interpreting results - Case study: Real-world scenarios and outcomes

Analyzing and Utilizing Recon Data (30 minutes) - Attack surface mapping is more than internet infrastructure - Introduction to the Open Asset Model (OAM) - Collecting email addresses with Amass - OAM types to be supported by the project - The Future of Mapping attack surfaces

Q&A Session (20 minutes)

Conclusion (10 minutes) - Recap of key takeaways - Additional resources and further learning - Closing remarks and feedback session

---

Preparation Requirements:** - Participants are encouraged to bring laptops with pre-installed OWASP Amass. - API keys for various data sources (details to be provided prior to the workshop).

Target Audience:** - Security researchers and professionals - Penetration testers - Network administrators - Anyone interested in improving their reconnaissance skills and knowledge

This workshop promises to be an engaging and educational experience, equipping attendees with the latest techniques and tools to enhance their security reconnaissance capabilities using OWASP Amass.

SpeakerBio: Jeff Foley
No BIO available

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Packet Detective
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Looking to upgrade your skills or see how you would fare in Capture The Packet? Come check out what Packet Detective has to offer! A step up in difficulty from Packet Inspector, Packet Detective will put your network hunting abilities to the test with real-world scenarios at the intermediate level. Take the next step in your journey towards network mastery in a friendly environment still focused on learning and take another step closer to preparing yourself for the competitive environment of Capture The Packet

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Packet Detective
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Looking to upgrade your skills or see how you would fare in Capture The Packet? Come check out what Packet Detective has to offer! A step up in difficulty from Packet Inspector, Packet Detective will put your network hunting abilities to the test with real-world scenarios at the intermediate level. Take the next step in your journey towards network mastery in a friendly environment still focused on learning and take another step closer to preparing yourself for the competitive environment of Capture The Packet

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Packet Detective
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Looking to upgrade your skills or see how you would fare in Capture The Packet? Come check out what Packet Detective has to offer! A step up in difficulty from Packet Inspector, Packet Detective will put your network hunting abilities to the test with real-world scenarios at the intermediate level. Take the next step in your journey towards network mastery in a friendly environment still focused on learning and take another step closer to preparing yourself for the competitive environment of Capture The Packet

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Packet Inspector
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

The perfect introduction to network analysis, sniffing, and forensics. Do you want to understand the techniques people use to tap into a network, steal passwords and listen to conversations? Packet Inspector is the place to develop these skills! For well over a decade, the Wall of Sheep has shown people how important it is to use end-to-end encryption to keep sensitive information like passwords private. Using a license of the world famous Capture The Packet engine from Aries Security, we have created a unique way to teach hands-on skills in a controlled real-time environment.

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Packet Inspector
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

The perfect introduction to network analysis, sniffing, and forensics. Do you want to understand the techniques people use to tap into a network, steal passwords and listen to conversations? Packet Inspector is the place to develop these skills! For well over a decade, the Wall of Sheep has shown people how important it is to use end-to-end encryption to keep sensitive information like passwords private. Using a license of the world famous Capture The Packet engine from Aries Security, we have created a unique way to teach hands-on skills in a controlled real-time environment.

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Packet Inspector
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

The perfect introduction to network analysis, sniffing, and forensics. Do you want to understand the techniques people use to tap into a network, steal passwords and listen to conversations? Packet Inspector is the place to develop these skills! For well over a decade, the Wall of Sheep has shown people how important it is to use end-to-end encryption to keep sensitive information like passwords private. Using a license of the world famous Capture The Packet engine from Aries Security, we have created a unique way to teach hands-on skills in a controlled real-time environment.

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 11:00-12:15 PDT

Title: Panel of Bug Bounty Community Leaders
When: Friday, Aug 9, 11:00 - 12:15 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

Join us for an engaging and insightful panel discussion at the Bug Bounty Village, where community leaders from four of the world's leading bug bounty platforms—HackerOne, Synack, YesWeHack, and Intigriti—come together to share their expertise and vision for the future of bug bounty programs. This panel, moderated by a prominent hacker from the community, will explore the latest trends, challenges, and innovations in the bug bounty space.

Attendees will gain valuable insights into how these platforms are evolving to meet the growing demands of cybersecurity, the strategies they employ to attract and retain top talent, and their perspectives on the impact of bug bounty programs on the broader security landscape. Through a crowdsourced Q&A session, community-driven questions will take center stage, allowing participants to delve into topics that matter most to them.

Whether you are a seasoned bug bounty hunter, a security professional, or someone new to the field, this panel offers a unique opportunity to learn from the leaders shaping the future of vulnerability disclosure and rewarding ethical hacking. Don't miss this chance to connect with industry pioneers and contribute to the dialogue that drives innovation and collaboration in cybersecurity.

Speakers: Inti De Ceukelaire,Jessica Sexton,Ryan Rutan,Lucas Philippe,Michael "codingo" Skelton,Roni "Lupin" Carta

SpeakerBio: Inti De Ceukelaire, Intigriti

Inti De Ceukelaire is a Belgian ethical hacker and cybercrime investigator. He currently works as the Chief Hacker Officer at Europe’s largest vulnerability disclosure platform, Intigriti, a founding member of the Hacker Policy Council. With extensive experience in the field of security and ethical hacking, Inti has earned a reputation as a thought leader in the industry. His work and expertise have been featured in a variety of international publications, including the BBC, Wired, The Verge, CNET, Mashable, and New York Magazine.

SpeakerBio: Jessica Sexton, HackerOne

Jessica Sexton, Sr. Director of Community at HackerOne, has significantly contributed over the past five years, leading the live hacking program and innovative initiatives like the Ambassador World Cup. She heads the Hacker Success Management team, focusing on retention, enablement, and growth of the hacker community. Before HackerOne, Jessica held roles in customer management and cybersecurity, honing her skills in strategy and growth. Her work inspires and energizes the HackerOne community, fostering a collaborative and inclusive environment.

SpeakerBio: Ryan Rutan, SynAck

After spending over a decade building online communities for tech savvy enterprises, Ryan has returned to his hacker roots as the Sr. Director, Community at the Synack Red Team. He is a long-time developer/maker at heart and technology innovator by trade, but his passion comes from uniting people, process and technology into sustainable community programs capable of scaling to meet any business challenge. In his spare time, he enjoys flexing his creativity by writing fiction novels (Fork This Life), hacking on IoT projects and furthering his cybersecurity knowledge through his programming, automation and integration talents cultivated over the past twenty years of his technical career.

SpeakerBio: Lucas Philippe, YesWeHack

BitK is a French Security Researcher, Bug Hunter, Member of the French CTF team The Flat Network Society and Tech Ambassador at YesWeHack. He has been doing CTF and bug bounty for over ten years with a specialty in web exploitation. He is also the author of multiple hacking tools like pwnfox, yesweburp, CTFNote and more.

SpeakerBio: Michael "codingo" Skelton, VP of Operations at Bugcrowd

Previously a top 10 bounty hunter at Bugcrowd, now the VP of Operations overseeing triage, appeals, escalations, and the support team, also creating YouTube content at youtube.com/codingo and developing tools at github.com/codingo.

SpeakerBio: Roni "Lupin" Carta, Co-Founder at Lupin & Holmes

Roni Carta, a.k.a @Lupin, is a 22 years old ethical hacker. He left school and his virtual classes to devote himself full-time to hacking. He credits Maurice Leblanc's book "Arsène Lupin" with immersing him into the culture and mindset of ethical hacking.

Roni co-founded with his brother Lupin & Holmes, an offensive security Research & Development company

---

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Password lab
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Follow real world password attack steps against a mock target in order to better understand how to protect yourself and improve the security of your passwords!

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Password lab
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Follow real world password attack steps against a mock target in order to better understand how to protect yourself and improve the security of your passwords!

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Password lab
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Follow real world password attack steps against a mock target in order to better understand how to protect yourself and improve the security of your passwords!

Return to Index - Add to Google - ics Calendar file

PYV - Friday - 16:30-16:59 PDT

Title: Payment Village CTF Day One Results
When: Friday, Aug 9, 16:30 - 16:59 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

Winners of Day One announced and prizes given out

Return to Index - Add to Google - ics Calendar file

PYV - Saturday - 16:30-16:59 PDT

Title: Payment Village CTF Day Two Results
When: Saturday, Aug 10, 16:30 - 16:59 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

Winners of Day Two announced and prizes given out

Return to Index - Add to Google - ics Calendar file

PYV - Saturday - 10:00-16:30 PDT

Title: Payment Village CTF
When: Saturday, Aug 10, 10:00 - 16:30 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

This year we have more challenges and more prizes!

Return to Index - Add to Google - ics Calendar file

PYV - Friday - 10:00-16:30 PDT

Title: Payment Village CTF
When: Friday, Aug 9, 10:00 - 16:30 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

This year we have more challenges and more prizes!

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 16:00-17:59 PDT

Title: Peer-to-Peer Mentoring and Networking with optional Swag, Pin & Sticker Exchange
When: Saturday, Aug 10, 16:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-04 - Map

Description:

Join us Women in Security and Privacy to mingle and network with privacy and security professionals. You can also bring some swag, pins, or stickers to exchange as part of the networking activities.

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Phisherman's Wharf - Phishing for Beginners
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Intuit R3DC0N's Phisherman's Wharf will lead beginners looking to learn how phishing campaigns are managed. This short introductory lab will give you hands on experience creating a phish test campaign from a cached email and web site using GoPhish, leverage email lists, and observe the responses when the victims interact with the phish emails in MailHog.

Accompanied by our expert guide, witness live hacking demonstrations showcasing the alarming simplicity behind breaching and controlling banned xIoT devices. Embrace the excitement. Join us at the Lab and let the hacking games begin!

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Phisherman's Wharf - Phishing for Beginners
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Intuit R3DC0N's Phisherman's Wharf will lead beginners looking to learn how phishing campaigns are managed. This short introductory lab will give you hands on experience creating a phish test campaign from a cached email and web site using GoPhish, leverage email lists, and observe the responses when the victims interact with the phish emails in MailHog.

Accompanied by our expert guide, witness live hacking demonstrations showcasing the alarming simplicity behind breaching and controlling banned xIoT devices. Embrace the excitement. Join us at the Lab and let the hacking games begin!

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Phisherman's Wharf - Phishing for Beginners
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Intuit R3DC0N's Phisherman's Wharf will lead beginners looking to learn how phishing campaigns are managed. This short introductory lab will give you hands on experience creating a phish test campaign from a cached email and web site using GoPhish, leverage email lists, and observe the responses when the victims interact with the phish emails in MailHog.

Accompanied by our expert guide, witness live hacking demonstrations showcasing the alarming simplicity behind breaching and controlling banned xIoT devices. Embrace the excitement. Join us at the Lab and let the hacking games begin!

Return to Index - Add to Google - ics Calendar file

AIV - Sunday - 10:00-10:59 PDT

Title: Photoshop Fantasies
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

The possibility of an altered photo revising history in a convincing way highlights a salient threat of imaging technology. After all, seeing is believing. Or is it? The examples history has preserved make it clear that the observer is more often than not meant to understand that something has changed. Surprisingly, the objectives of photographic manipulation have remained largely the same since the camera first appeared in the 19th century. The old battleworn techniques have simply evolved to keep pace with technological developments. In this talk, we will learn about the history of photographic manipulation, from the invention of the camera to the advent of generative AI. Importantly, we will consider the reception of photo editing and its relationship to the notion of reality, which is more significant than the technologies themselves. Surprisingly, we will discover that creative myth making has found a new medium to embed itself in. This talk is based on Walter Scheirer's recent book A History of Fake Things on the Internet (Stanford University Press 2023).

SpeakerBio: Walter Scheirer, University of Notre Dame
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: PhreakMe presented by HackedExistence
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-C - Map

Description:

The contest will be hosted on the Publicly Switched Telephone Network and will be live for access 24/7, with real world PSTN phone numbers to dial into.

The Hacked Existence team will be hosting a telecom based CTF. The CTF will be hosted on live VoIP lines routed through a modified asterisk PBX. This will allow participants to dial in to the CTF from a real world telephone routable phone number allowing them to hunt the PBX for flags. The flags will be based around utilizing historically accurate tactics, techniques, and procedures to manipulate emulated old school switching systems.

The purpose of our contest is to bring awareness around the still existing weaknesses in our telecom infrastructure and Interactive Voice Response Systems. Ideally visitors to our contest area will participate in the CTF allowing them to get a better understanding of telecom hacking in the year 2024 as well as a respect for the art of phreaking from yesteryears.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: PhreakMe presented by HackedExistence
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-C - Map

Description:

The contest will be hosted on the Publicly Switched Telephone Network and will be live for access 24/7, with real world PSTN phone numbers to dial into.

The Hacked Existence team will be hosting a telecom based CTF. The CTF will be hosted on live VoIP lines routed through a modified asterisk PBX. This will allow participants to dial in to the CTF from a real world telephone routable phone number allowing them to hunt the PBX for flags. The flags will be based around utilizing historically accurate tactics, techniques, and procedures to manipulate emulated old school switching systems.

The purpose of our contest is to bring awareness around the still existing weaknesses in our telecom infrastructure and Interactive Voice Response Systems. Ideally visitors to our contest area will participate in the CTF allowing them to get a better understanding of telecom hacking in the year 2024 as well as a respect for the art of phreaking from yesteryears.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: PhreakMe presented by HackedExistence
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-C - Map

Description:

The contest will be hosted on the Publicly Switched Telephone Network and will be live for access 24/7, with real world PSTN phone numbers to dial into.

The Hacked Existence team will be hosting a telecom based CTF. The CTF will be hosted on live VoIP lines routed through a modified asterisk PBX. This will allow participants to dial in to the CTF from a real world telephone routable phone number allowing them to hunt the PBX for flags. The flags will be based around utilizing historically accurate tactics, techniques, and procedures to manipulate emulated old school switching systems.

The purpose of our contest is to bring awareness around the still existing weaknesses in our telecom infrastructure and Interactive Voice Response Systems. Ideally visitors to our contest area will participate in the CTF allowing them to get a better understanding of telecom hacking in the year 2024 as well as a respect for the art of phreaking from yesteryears.

Return to Index - Add to Google - ics Calendar file

QTV - Sunday - 10:00-10:59 PDT

Title: Physical Fundamentals of Quantum Computing
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:
SpeakerBio: Erez M Abrams

My name is Erez Abrams and I'm currently a physics and math undergraduate student at MIT with four years' experience in research on the mechanism underlying controlled quantum systems. Prior to burying myself in the ungodly mess that is quantum field theory, I often lectured at or ran cybersecurity, math, and physics teams/clubs for high schoolers and undergraduates, and I was an avid player of CTFs. Nowadays, I mostly sit in a dark room ruminating over a whiteboard full of Feynman diagrams in the hopes of understanding something or other about how the universe functions, but I still passionately love to teach and am very excited to share my knowledge with the wonderful attendees of DEF CON 32's Quantum Village!

Return to Index - Add to Google - ics Calendar file

PSV - Sunday - 11:00-11:30 PDT

Title: Physical OSINT
When: Sunday, Aug 11, 11:00 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Open source intelligence may sound like something you've never done, but even something as simple as finding your old friends on social media overlaps with skills required for the job. Learn about what OSINT is, how to start an investigation, and resources used by experts to collect the maximum amount of data on a facility before ever visiting the site.

SpeakerBio: Lukas McCullough

Lukas recently graduated from Marist College, majoring in cybersecurity; and will be continuing his education at Boston University toward a Masters of Criminal Justice in Cybercrime Investigation & Cybersecurity and Crime Analysis. In his free time, he competes in CTFs and rock climbs from time to time.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 10:00-10:50 PDT

Title: Physical Red Teaming for Offensive Cyber Teams
When: Saturday, Aug 10, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Offensive security is an unfamiliar concept to most physical security practitioners. Yet we still rely on physical security teams to protect our hardware, network, ports, and assets. Physical security professionals are often non-technical, former law enforcement/military, and are focused on protecting people instead of property. This talk will bridge the gap between physical and cyber red teaming, covering the best approaches, common pitfalls, dangers, and benefits of testing physical security programs as part of a red team assessment. From the difficulty of “patching” physical vulnerabilities to examples of red teams gone wrong and how to approach physical security teams without being viewed as an actual adversary - you will walk away with a broader perspective and the ability to be a better partner when conducting physical red team assessments.

Speakers: Shawn Abelson,Ana Aslanishvili

SpeakerBio: Shawn Abelson
No BIO available
SpeakerBio: Ana Aslanishvili
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 14:00-14:50 PDT

Title: Physical Security - Bypassing Access Control Systems
When: Friday, Aug 9, 14:00 - 14:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

Breaking Through Barriers: Attacking Access Control Systems

In this in-depth session, we will dive into the vulnerabilities of access control systems, specifically targeting RFID readers and the Wiegand protocol that these readers commonly use to interact with other security devices. Discover the intricate design process behind a custom tool crafted to exploit specific Schlage proximity readers.

This talk will cover:

- The fundamental weaknesses in RFID reader technologies and the Wiegand communication protocol.
- Step-by-step breakdown of designing a tool to man-in-the-middle Schlage proximity readers.
- Real-world implications and case studies demonstrating successful attacks on high-security installations.

Attendees will gain actionable insights into the inner workings of access control systems, enabling them to conduct physical security assessments with more success. This session is a must-attend for security professionals looking to stay ahead of the curve in physical offensive security strategies.

SpeakerBio: Andrew Johnson

No BIO available

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 14:00-14:30 PDT

Title: Physical Security Assessment Basics for Internal Employees
When: Friday, Aug 9, 14:00 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

If you have an interest in physical security and want to help your employer secure their buildings, this talk is for you! We'll cover common flaws in locks, alarms, surveillance systems and employee training, and how to test for them and suggest remediations to company leadership. Learn methods of lock bypass, alarm bypass, forcible entry, social engineering and other common vulnerabilities!

This talk is aimed at employees whose primary job function does not involve physical security - that often includes cybersecurity teams though, so we'll make lots of analogies to infosec concepts, but the talk is accessible to everyone.

SpeakerBio: Billy Graydon, Principal at GGR Security

Bill Graydon is a principal at GGR Security, where he hacks everything from locks and alarms to critical infrastructure; this has given him some very fine-tuned skills for breaking stuff. He’s passionate about advancing the security field through research, teaching numerous courses, giving talks, and running the Physical Security Village at various cons. He’s received various degrees in computer engineering, security, and forensics and comes from a broad background of work experience in physical and cyber security, anti-money laundering, and infectious disease detection.

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 10:00-17:59 PDT

Title: Physical Security Village Activities
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

The Physical Security Village explores the world of hardware bypasses and techniques generally outside of the realm of cyber-security and lockpicking. Come learn some of these bypasses, how to fix them, and have the opportunity to try them out for yourself.

We'll be covering the basics, like the under-the-door-tool and latch slipping attacks, as well as an in depth look at more complicated bypasses. Learn about elevator hacking, attacking alarm systems at the sensor and communication line, and cut-away and display models of common hardware to show how it works on the inside.

Looking for a challenge? Show us you can use lock bypass to escape from a pair of standard handcuffs in under 30 seconds and receive a prize!

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 10:00-17:59 PDT

Title: Physical Security Village Activities
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

The Physical Security Village explores the world of hardware bypasses and techniques generally outside of the realm of cyber-security and lockpicking. Come learn some of these bypasses, how to fix them, and have the opportunity to try them out for yourself.

We'll be covering the basics, like the under-the-door-tool and latch slipping attacks, as well as an in depth look at more complicated bypasses. Learn about elevator hacking, attacking alarm systems at the sensor and communication line, and cut-away and display models of common hardware to show how it works on the inside.

Looking for a challenge? Show us you can use lock bypass to escape from a pair of standard handcuffs in under 30 seconds and receive a prize!

Return to Index - Add to Google - ics Calendar file

PSV - Sunday - 10:00-12:59 PDT

Title: Physical Security Village Activities
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

The Physical Security Village explores the world of hardware bypasses and techniques generally outside of the realm of cyber-security and lockpicking. Come learn some of these bypasses, how to fix them, and have the opportunity to try them out for yourself.

We'll be covering the basics, like the under-the-door-tool and latch slipping attacks, as well as an in depth look at more complicated bypasses. Learn about elevator hacking, attacking alarm systems at the sensor and communication line, and cut-away and display models of common hardware to show how it works on the inside.

Looking for a challenge? Show us you can use lock bypass to escape from a pair of standard handcuffs in under 30 seconds and receive a prize!

Return to Index - Add to Google - ics Calendar file

PLV - Saturday - 12:30-13:15 PDT

Title: Pick Your Poison: Navigating a secure clean energy transition
When: Saturday, Aug 10, 12:30 - 13:15 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Clean Energy technology, while essential for the energy transition, often utilizes components sourced from adversarial countries, potentially increasing cyber vulnerabilities, especially in systems managed by smaller utilities with limited cybersecurity expertise. The previous approaches of 'rip and replace' to eliminate foreign components have proved inadequate and if applied to clean energy, may be economically and technically destabilizing.

This policy session will also delve into the broader implications of a digitalized supply chain, where simplistic views of cybersecurity do not suffice. Instead, a nuanced understanding of the operational and physical realities of energy systems is essential. By discussing how to balance immediate economic pressures against long-term sustainability and security, the session aims to foster a more informed and effective policy discourse.

In summary, as the energy sector evolves to include diverse infrastructure systems—ranging from hospitals to military installations—the need for a robust, informed, and agile policy approach to cybersecurity becomes increasingly critical. This session will provide a platform for critical discourse to ensure that the transition to renewable energy is both secure and sustainable, aligning climate goals with national security imperatives

SpeakerBio: Emma Stewart, Chief Power Grid Scientist at Idaho National Labs

Emma M. Stewart, Ph.D., is a respected power systems security specialist with expertise in power distribution and operational cybersecurity. Emma is currently the Chief Power Grid Scientist at Idaho National Labs and the Director of the Center for Securing the Digital Energy Transition.

From 2021 to 2023, Dr. Stewart served as the Chief Scientist at the National Rural Electric Cooperative Association (NRECA), where she led NRECA Research and the Co-Op Cyber Program. Her responsibilities included providing electric cooperatives with education, training, information sharing, incident support, technology integration, and R&D services. At Lawrence Livermore National Laboratory, she served as the Associate Program Leader for Cyber and Infrastructure Resilience, managing research on prevention and response to high consequence grid events such as wildfire and cyber attack. At Lawrence Berkeley National Laboratory, she was the Deputy Group Leader in the Grid Integration Group and played a major role in developing the first micro-synchrophasor network in the US enabling the data to be used to prevent wildfire and equipment failure.

Before joining national laboratories, Dr. Stewart worked as a Senior Engineer at BEW Engineering, where she led distribution planning, modeling, and analysis consulting for large utility customers in Hawaii and California. Dr. Stewart has made significant contributions to the field of security of power systems, receiving patents for innovations in power distribution systems and data analytics, and is one of the few who truly works at the center of the clean energy, energy security and cybersecurity venn diagram.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Pinball High Score Contest
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-A - Map

Description:

The inaugural Pinball High Score contest at DEF CON will run Friday and Saturday:

Achieving a high score may sound simple but pinball rulesets are very complex and the skill to complete a “Wizard Mode” or achieve a high score requires research, practice, knowledge and execution. Out of the box thinking, analytical skills and pattern recognition are traits that pinball players must exhibit to be successful and some games have rule sets that can be studied and exploited to achieve a high score. Hackers are at an advantage here and while this is just a pinball contest, I expect that the community is ready for this challenge.

Stern Pinball has prepared an exclusive DEF CON 32 digital badge that will be available for any attendee to earn for playing in this event. Additional DEF CON specific Insider Connect badges may be unlocked during game play.

Pinball developers have a long history of including Easter Eggs/COWS in games. Easter eggs “may” also be available for attendees to discover during the conference. Undocumented Easter eggs found by players during the event will be documented, verified and recognized.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Pinball High Score Contest
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-A - Map

Description:

The inaugural Pinball High Score contest at DEF CON will run Friday and Saturday:

Achieving a high score may sound simple but pinball rulesets are very complex and the skill to complete a “Wizard Mode” or achieve a high score requires research, practice, knowledge and execution. Out of the box thinking, analytical skills and pattern recognition are traits that pinball players must exhibit to be successful and some games have rule sets that can be studied and exploited to achieve a high score. Hackers are at an advantage here and while this is just a pinball contest, I expect that the community is ready for this challenge.

Stern Pinball has prepared an exclusive DEF CON 32 digital badge that will be available for any attendee to earn for playing in this event. Additional DEF CON specific Insider Connect badges may be unlocked during game play.

Pinball developers have a long history of including Easter Eggs/COWS in games. Easter eggs “may” also be available for attendees to discover during the conference. Undocumented Easter eggs found by players during the event will be documented, verified and recognized.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Pinball High Score Contest
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-01-A - Map

Description:

The inaugural Pinball High Score contest at DEF CON will run Friday and Saturday:

Achieving a high score may sound simple but pinball rulesets are very complex and the skill to complete a “Wizard Mode” or achieve a high score requires research, practice, knowledge and execution. Out of the box thinking, analytical skills and pattern recognition are traits that pinball players must exhibit to be successful and some games have rule sets that can be studied and exploited to achieve a high score. Hackers are at an advantage here and while this is just a pinball contest, I expect that the community is ready for this challenge.

Stern Pinball has prepared an exclusive DEF CON 32 digital badge that will be available for any attendee to earn for playing in this event. Additional DEF CON specific Insider Connect badges may be unlocked during game play.

Pinball developers have a long history of including Easter Eggs/COWS in games. Easter eggs “may” also be available for attendees to discover during the conference. Undocumented Easter eggs found by players during the event will be documented, verified and recognized.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 16:00-16:50 PDT

Title: Pipeline Pandemonium: How to Hijack the Cloud and Make it Rain
When: Saturday, Aug 10, 16:00 - 16:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

In today's tech landscape, where cloud computing and DevOps practices have converged, managing the integrity of CI/CD pipelines is essential. These intertwined elements should be holistically addressed, particularly regarding security measures.

However, with the rise of automation, there comes an increased risk. Join us for "Pipeline Pandemonium," a comprehensive talk about vulnerabilities within CI/CD pipelines and their potential to inadvertently negatively affect organizations that rely on cloud environments. Through real-world examples and case studies, attendees will explore the convergence of rapid software delivery and cloud infrastructure, uncovering the methods used by malicious actors to infiltrate pipelines and compromise cloud security.

Several real-world examples will be expounded, including code injection, dependency hijacking, unauthorized access through over-provisioned keys, runner abuse, and artifact poisoning. More specifically, much of the talk will focus on common techniques to abuse privileges and configurations associated with GitHub actions, CircleCI and Jenkins pipelines. The presenter has real world experience exploiting these issues at fortune 500 companies and has made significant contributions to their security organization’s security posture.

Attendees will gain a deep understanding of the vulnerabilities inherent in CI/CD processes and general strategies to defend against common attacks. Although the focus of the presentation is for a broad audience and requires no in-depth knowledge about the specific topics that will be covered.

Join us for "Pipeline Pandemonium" and discover how to navigate the turbulent waters of cloud security with confidence, turning the tide against insecurity and reclaiming control of your CI/CD pipelines.

SpeakerBio: Blake Hudson

No BIO available

Return to Index - Add to Google - ics Calendar file

XRV - Sunday - 10:00-11:59 PDT

Title: Play All the Things
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

Play VR the gear comes out for a casual, hands on demo area to explore the metaverse in VR with games & expoloration in Meta Quest VR and Meta Raybans MR

Return to Index - Add to Google - ics Calendar file

Title: Play by Play of the Curling v. Raffensperger Lawsuit
When: Friday, Aug 9, 10:45 - 11:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

For three weeks in January 2024, a federal judge heard arguments that Ballot Marking Devices (BMDs) as they are uniformly used in Georgia burden the right to vote to the extent that their continued use is unconstitutional. In 2019, the same court banned the use of Direct Recording Equipment (DRE) on the same grounds. Banning BMDs would have national repercussions. The case was litigated in a bench trial, a lawsuit not tried in front of a jury.

Using actual court presentations and documents, the proposed panel will summarize the arguments made by attorneys and experts for the Plaintiffs (a coalition of cybersecurity and voting systems experts and voting rights activists) and the Defendant (Georgia Secretary of State Raffmsperger). Panelists include representatives of the plaintiffs, defendants, and independent experts, moderated by a distinguished legal journalist. Observers will explain the extraordinary coincidences surrounding this lawsuit, including the events of January 6th, the Trump allies' successful efforts to steal the state's software, and the attempt by backers of then-President Donald Trump and the attempt to brand Plaintiffs as election deniers. Panelists will also recreate technical demonstrations used in court.

The panel will use a novel "steelman" analysis of the Defense's arguments. Unlike strawman analysis, a steelman (often called charitable analysis) argument crafts the most favorable interpretation of the responses to the Plaintiff's complaint, strengthening and in some cases correcting errors.

Speakers: Susan Greenhalgh,Mary Kaiser,Drew Springall,Philip Stark

SpeakerBio: Susan Greenhalgh

Susan Greenhalgh is the Senior Advisor on Election Security for Free Speech For People. Ms. Greenhalgh has previously served as vice president of programs at Verified Voting and at the National Election Defense Coalition, advocating for secure election protocols, paper ballot voting systems and post-election audits. Recognized as an expert on election security, she has been invited to testify before the U.S. Commission on Civil Rights and has been an invited speaker at meetings of the MITRE Corporation, the National Conference of State Legislatures, the Mid-West Election Officials Conference, the International Association of Government Officials, the Election Verification Network and the E-Vote-ID conference in Bregenz, Austria. She is a frequent source for reporters from The New York Times, The Washington Post, The

Wall Street Journal, Politico, USA Today, Associated Press, National Public Radio and other leading news outlets. She has appeared on CNN and MSNBC's The Rachel Maddow Show, and various other television news shows. She has a BA in Chemistry from the University of Vermont.

SpeakerBio: Mary Kaiser

Mary Kaiser is a partner in Goodwin's Antitrust and Competition practice and a member of the firm's Complex Litigation & Dispute Resolution practice. Mary represents domestic and multinational companies as both plaintiffs and defendants in antitrust and competition-related matters, including federal and state court proceedings, arbitrations, and government antitrust enforcement proceedings.

SpeakerBio: Drew Springall

Drew Springall is an assistant professor of computer science at Auburn University. He served as an expert to the plaintiffs in the Curling v. Raffensperger case, and received access by court order to conduct a security assessment of Georgia's

touchscreen ballot marking devices.

SpeakerBio: Philip Stark

Philip B. Stark is Distinguished Professor of Statistics at the University of California, Berkeley, where he currently focuses on methodology and applications in physical, life, and social sciences. In 2007, he invented risk limiting audits, endorsed by the National Academies of Science, Engineering, and Medicine and the American Statistical Association, among others, and is now required or authorized by law in about 15 states.

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 14:45-15:30 PDT

Title: Playing with Quantum: wayfinding with quantum game theory
When: Saturday, Aug 10, 14:45 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

The global quantum community is searching for future applications of quantum computing and quantum communications. A somewhat uncommon way to think about this problem is through quantum game theory. This field of research looks at how quantum resources can be used in both cooperative and competitive games to achieve what would be impossible with only classical resources. In this talk we'll look at some of the fundamentals of quantum game theory, including some archetypal examples of quantum strategies and some theoretical results that show how quantum games differ from classical ones.

SpeakerBio: Michael Dascal

Michael leads the FCAT quantum computing incubator and is responsible for monitoring the quantum ecosystem and exploring collaboration, engagement, and community development opportunities. He has given multiple technical and non-technical talks in quantum computing and quantum information, and is dedicated to promoting an optimistic, but realistic understanding of quantum technologies and the quantum timeline.

Michael's background includes a combination of industry and academic experience, including a decade in marketing and communications for Fortune 100 brands. He holds a PhD in foundations of quantum mechanics and quantum information and degrees in philosophy, physics, and linguistics.

Return to Index - Add to Google - ics Calendar file

QTV - Sunday - 12:00-12:59 PDT

Title: Policy and the Quantum: Where do we start?
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 18:30-22:30 PDT

Title: Policy Mixer @ DEF CON
When: Friday, Aug 9, 18:30 - 22:30 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 18:30-22:30 PDT

Title: Policy Mixer @ DEF CON
When: Saturday, Aug 10, 18:30 - 22:30 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

Return to Index - Add to Google - ics Calendar file

CPV - Sunday - 10:00-10:30 PDT

Title: Porn & Privacy
When: Sunday, Aug 11, 10:00 - 10:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

As our social lives are highly intertwined with our online lives, people share a lot of information and create pictures and content that needs to be secured. In this talk I cover obscenity laws, revenge porn (nonconsensual distribution of intimate images), stalking, catfishing and sextortion and how people can prevent information being leaked as well as how to recover from it.

SpeakerBio: ET

ET is a cybersecurity professional who cares about digital privacy. They have helped people who have been affected by revenge pornography and help them put together a plan of action. I like to volunteer, I help with BSides Orlando, DEATHCon and DC407.

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 11:00-11:59 PDT

Title: Power To The Purple
When: Saturday, Aug 10, 11:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

The modern cybersecurity realm is no longer one where defenders can work in a vacuum and be successful. Conversely, many people are starting to lose faith in the value of penetration testing as a mechanism to measure their organizational security posture. A collaborative milestone driven approach where Red and Blue teams operate in tandem, is necessary to ensure a proactive approach to enhancing the security of our organizations. This is where Purple Teaming comes into play. In this 2-hour hands-on workshop you will be introduced to Purple Team Exercises and play the role of a Cyber Threat Intelligence analyst, Red Team operator, and Blue Team security analyst. We have set up an isolated environment for each attendee to go through a Purple Team Exercise following the Purple Team Exercise Framework (PTEF). This event will give participants a chance to test out new tools, techniques, and procedures learned during the workshop.

Speakers: Tyler Casey,Trey Bilbrey

SpeakerBio: Tyler Casey, Deputy of SCYTHE Labs

Tyler Casey is a seasoned Cyber Professional with over a decade of experience in Defensive Cyber Operations (DCO). Currently serving as Detection Engineer and Deputy at Scythe Labs, Tyler specializes in developing and implementing robust defensive cybersecurity measures to detect and mitigate evolving threats. Prior to joining SCYTHE, Tyler worked in DCO Operations for the U.S. Government, both as a Federal Civilian and Active-Duty Marine. During that tenure, Tyler deployed internationally in support of incident response and targeted threat hunting. Throughout his career, he has been dedicated to enhancing cyber defenses, ensuring the security of critical systems, and contributing to the broader cybersecurity community.

SpeakerBio: Trey Bilbrey, Lead at SCYTHE Labs

Trey Bilbrey is the Lead of SCYTHE Labs, specializing in Purple Team Exercises, Threat Emulation, Critical Infrastructure, and holistic cyber operations. Trey's 15+ years of industry experience has allowed him to become an excellent educator, defender of networks, and a cultivator of cybersecurity professionals. Prior to joining SCYTHE, Trey held positions at notable organizations such as Hack The Box (HTB Academy content Developer), The Army Corps of Engineers (ICS/SCADA Penetration Testing), and a veteran of the United States Marine Corps (Defensive and Offensive Cyber Operations). Current certifications include the CISSP, GICSP, GCIP, and K>FiveFour RTAC.

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 10:00-10:59 PDT

Title: Practical Exploitation of DoS in Bug Bounty
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

The talk "Practical Exploitation of DoS in Bug Bounty" explains methods for identifying and exploiting Denial of Service (DoS) vulnerabilities in bug bounty programs. Starting with an overview of DoS attacks and their impact, we will highlight how these attacks disrupt services by overwhelming resources or exploiting flaws. The talk covers various DoS attack types, including N+1 errors, in-depth GraphQL crashing, and Cache Poisoning, with real-world examples demonstrating their effects.

We will then detail practical techniques for discovering DoS vulnerabilities. This includes automated scanning tools, manual testing methods, and understanding the target system's architecture.

N+1 errors occur when an application makes redundant database queries, significantly impacting performance. Attackers can exploit this by triggering numerous unnecessary queries, causing severe slowdowns or crashes. GraphQL, a query language for APIs, can be vulnerable to complex queries that consume excessive resources, leading to server crashes. We will show how to craft such queries and the resulting impact. Cache Poisoning involves manipulating cached data to serve malicious or incorrect content, which can disrupt services or degrade performance. We will explore techniques to poison caches and demonstrate the potential consequences.

Additionally, the talk emphasizes the importance of responsibly reporting discovered vulnerabilities to bug bounty programs. Best practices are shared for effectively communicating findings and ensuring timely mitigation. Of course, there are some fails during this path, and those are going to be covered too.

The session wraps up by stressing the need for continuous learning and staying updated on the latest trends in DoS attack vectors and mitigation strategies

SpeakerBio: Roni "Lupin" Carta, Co-Founder at Lupin & Holmes

Roni Carta, a.k.a @Lupin, is a 22 years old ethical hacker. He left school and his virtual classes to devote himself full-time to hacking. He credits Maurice Leblanc's book "Arsène Lupin" with immersing him into the culture and mindset of ethical hacking.

Roni co-founded with his brother Lupin & Holmes, an offensive security Research & Development company

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 11:00-11:59 PDT

Title: Prendendo Fraudadores utilizando Técnicas de Red Team
When: Friday, Aug 9, 11:00 - 11:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Esta palestra apresenta um estudo de caso real onde técnicas de Red Team foram cruciais para identificar e prender uma quadrilha de fraudadores especializada em esquemas financeiros. A equipe de Red Team conduziu simulações de ataques controlados, explorando vulnerabilidades na segurança da organização alvo.

SpeakerBio: Gustavo Roberto, Old Pirate

As a seasoned Information Security professional with over a decade of experience in the industry, I have developed a deep expertise in Red Team and Penetration Testing. I am highly skilled in identifying and mitigating security vulnerabilities, and I take a proactive approach to helping organizations defend against cyber threats.

Return to Index - Add to Google - ics Calendar file

Title: Preparing for the Future: A Discussion of our Rapidly Evolving Threat Landscape
When: Friday, Aug 9, 13:00 - 13:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Seems like the world has completely changed in the last 12-24 months:

- Multiple Global Conflicts
- Launch of ChatGPT
- CISO's being held personally accountable for security breaches
- Government Regulations on security
- Economic Uncertainties (interest rates, layoffs)

All of these changes have played a major role in reshaping the security landscape. From adversaries with political motivations to another just trying to provide for his/her family. Security is no longer just your job, but you could actually be held personally liable. Oh and don't forget that an adversary now has the ability to rewrite vulnerabilities with the click of a button, or can create deep fakes so real that a zoom call with multiple "people" was undetectable by a real person.

Speakers: Jamie Hardy,Rachael Tubbs,Steve McGregory ,Ted Harrington

SpeakerBio: Jamie Hardy, Principal Product Manager at Intuit

Jamie Hardy is a Principal Product Manager at Intuit responsible for Adversary Management. He's spent 14 years in the industry with a background as a software and cyber security engineer. He's worked in fintech, government, and semiconductor spaces making the transition from engineering to Product Management when taking on IoT security at Qualcomm. He likes to break things, build things, and is passionate about bringing new products to reality, which makes him a swiss army knife for cybersecurity product management. You may catch him on the slopes, at the links, or leading security conferences. He enjoys family time with his wife, young baby son, two vizslas, all while rocking Hawaiian shirts.

SpeakerBio: Rachael Tubbs

Rachael Tubbs is the village lead of IoT Village. She is currently working on her PhD in Forensic Psychology where she is studying the world of ethical hacking and the mindset of hackers. She has presented at Hack the Capitol and RSA Conference.

SpeakerBio: Steve McGregory , Senior Director of the Cybersecurity Center of Excellence (COE) at Keysight Technologies

Steve McGregory is Senior Director of the Cybersecurity Center of Excellence(COE) at Keysight Technologies. The Cybersecurity COE researches cyber threats and gathers actionable intelligence. Steve has over three decades of experience working in computer and network security. Steve's work experience has covered all aspects of cybersecurity, from operational security practices such as defending an Internet Service Provider business, building security controls at TippingPoint(now Trend Micro), and, most recently, building cybersecurity test solutions at Keysight Technologies. Steve is passionate about cybersecurity and focuses his professional work on educating people about and protecting them from cyber-attacks.

SpeakerBio: Ted Harrington, Executive Partner at Independent Security Evaluators

Ted Harrington is the Executive Partner at Independent Security Evaluators and the number one bestselling author of Hackable. He's helped hundreds of companies fix tens of thousands of security vulnerabilities, including Google, Amazon, and Netflix. Ted has been featured in more than 100 media outlets, including The Wall Street Journal, Financial Times, and Forbes.

SEV - Saturday - 17:30-17:59 PDT

Title: Presentation: It Takes a Village...
When: Saturday, Aug 10, 17:30 - 17:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Its time to ask the question: “Where do we go from here?” Join SEC Village founders, Snow & JC to have a heart to heart about how we shape the future of the SEC. If you’re looking for how to get involved, or have ideas for the village, be here! We need you and want to hear from you!

Return to Index - Add to Google - ics Calendar file

SEV - Friday - 17:15-17:59 PDT

Title: Presentation: The 2024 #SECVC Debrief
When: Friday, Aug 9, 17:15 - 17:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Join the Founders of the Social Engineering Community as they break down this year's Vishing Competition (#SECVC). They'll talk about how the competition is organized, and some of the big takeaways, trends, and surprises (both good and bad) from the OSINT and Vishing Plan reports. They'll also recount some of the highlights from this year's live calls.

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 16:00-16:50 PDT

Title: Product security considerations for OT security appliances
When: Saturday, Aug 10, 16:00 - 16:50 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The adoption of OT security solutions into the world's most critical infrastructure has increased dramatically. The location in which these appliance reside within control networks poses unique risk as both management interfaces and even more often monitoring interfaces reside within segments that contain critical process automation equipment. This talk will explore essential product security considerations specific to OT security appliances, secure deployment strategies, device and network hardening techniques, and some real-world examples of discovered vulnerabilities in COTS appliances.

Speakers: Brandon Dudley,Robert Landavazo

SpeakerBio: Brandon Dudley, Field Operations Engineer at Dragos

Brandon Dudley is a Field Operations Engineer at Dragos, with 10 years of cybersecurity experience. Brandon deploys and configures the Dragos platform in OT networks, working with numerous critical infrastructure sectors. He was formerly an incident responder as well as a researcher specializing in PLC exploitation at a systems security lab. He has previously published on OT honeypots and has generated numerous honeypot datasets.

SpeakerBio: Robert Landavazo, Senior Director of Solution Architects at Dragos

Robert Landavazo is a Senior Director of Solution Architects at Dragos, he has more than 18 years of experience in cybersecurity, 12 of the most recent working in OT roles. Most recently, Robert’s focus has been on building world class teams of Solution Architects at Dragos and previously at security and configuration management software company with a global presence. Earlier in his career, Robert was an industrial cybersecurity practitioner in the electric utility sector, responsible for implementing the NERC Critical Infrastructure Protection (CIP) internal compliance program and securing distribution, transmission, and generation assets across the western US.

Return to Index - Add to Google - ics Calendar file

CHV - Saturday - 16:30-16:59 PDT

Title: Programming a CTS-V Gauge Cluster into an ATS-V, out of pure spite
When: Saturday, Aug 10, 16:30 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Some cars are over-engineered, some are too basic, and some check every box except one. I did that research over months when trying to buy a new car, and landed on a 6MT Cadillac ATS-V while only wanting and dealing with Japanese cars, specifically Lexus/Toyota. The one thing it was missing was a digital gauge cluster, and programmers were asking $350, so I set off to figure it out myself. I then dove deep into GM electronics and programming, found a smart dude who initially cracked it all for free to spite all the money-grabbing gatekeepers, then became a hyprocrite, backtracking asking thousands to reveal his learnings. This presentation will go over how I programmed that cluster, posted everything on Github, out of spite.

SpeakerBio: Varjitt Jeeva, Software Engineer

Software Engineer with a love of tuner cars and car electronics

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:30-11:30 PDT

Title: Protecting the Backbone of Our Modern World
When: Saturday, Aug 10, 10:30 - 11:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

In today's volatile geopolitical landscape, the security of critical infrastructure—such as power grids, water supplies, and transportation systems—has never been more important. As global tensions rise, these vital systems increasingly become targets for cyber threats from state and non-state actors alike. This talk will delve into the evolving landscape of cyber threats targeting these essential services, highlighting notable attacks and their devastating impacts. We will explore the methodologies employed by malicious actors, including advanced persistent threats and ransomware, and examine real-world case studies to understand the stakes involved. The discussion will also cover the latest strategies and technologies for protecting critical infrastructure, emphasizing a defense-in-depth approach.

SpeakerBio: Soledad Antelada Toledano, Google -Office of the CISO

Soledad Antelada Toledano is the Security Technical Program Manager at Google. She previously worked for Berkeley Lab, one of the most prestigious scientific centers in the world and one of the first nodes of ARPANET, the forerunner of the Internet. Soledad was the first woman in the history of the Cybersecurity department at Berkeley Lab. After specializing in 'penetration testing' for several years, Soledad also develops research and advancement tasks for intrusion detection systems, monitoring of high capacity networks and vision and research exercises on how cybersecurity will evolve in the next 10 years adopting techniques of Artificial Intelligence for intrusion detection and handling of BigData generated by monitoring tools. Soledad has combined her work at the Berkeley lab in recent years with the responsibility of being the head of security for the ACM / IEEE Supercomputing Conference, the annual supercomputing conference in the United States, protecting and building the network architecture of SCinet, the fastest network in the world. She is the founder of GirlsCanHack, an organization dedicated to engaging women in the cybersecurity field, encouraging women to pursue a career in cybersecurity Soledad was named one of the 20 Most Influential Latinos in Technology in America in 2016. She has recently joined Google as a Technical Program Manager for Security. Soledad has recently published the book Critical Infrastructure Security: Cybersecurity lessons learned from real-world breaches

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 15:00-16:30 PDT

Title: Prototype Pollution in Depth, From Beginner to 0-Day Hunter
When: Friday, Aug 9, 15:00 - 16:30 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

Prototype pollution is a vulnerability in JavaScript applications that can have varying impacts depending on the complexity and nature of the affected app. By manipulating an object's prototype chain, an attacker can introduce malicious properties, leading to unexpected behavior and potentially allowing the attacker to execute arbitrary code. In this workshop, we will first try to understand the subtleties of the Javascript prototype chain. Then, we will explore different techniques for black box detection. Finally, we will use pp-finder to find new RCE gadgets in popular libraries.

Pre-Requisites: - Attendees are expect to have basic Javascript knowledge and have a computer with docker ready

SpeakerBio: Lucas Philippe, YesWeHack

BitK is a French Security Researcher, Bug Hunter, Member of the French CTF team The Flat Network Society and Tech Ambassador at YesWeHack. He has been doing CTF and bug bounty for over ten years with a specialty in web exploitation. He is also the author of multiple hacking tools like pwnfox, yesweburp, CTFNote and more.

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:30-11:15 PDT

Title: Psychic Paper: Making eink access badges accessible for anyone
When: Saturday, Aug 10, 10:30 - 11:15 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

To make RFID access badges vendors in China have created eink badges where instead of printing a badge out you instead program the eink portion of the badge with an smartphone app and then program the RFID portion. At this time the ones that are sold are either black and white or black and white and red. There is no security implemented so all you need to do is download the app to reprogram the front of the badge. This makes anyone able to reprogram both the front and back of the badge.

SpeakerBio: Joshua Herman

My day job is that I am a release engineer specializing in compliance of various vendors at a large bank. Hacking, LLMs, and open source development are hobbies that I have. I have many given many talks such as at Defcon 31 about a natural language security scanner, Thotcon about of large scale social engineering, pyOhio about making chatbots using Blenderbot from Facebook, and at the Chicago Python User group about Cellular Automata I found in college (Snowlife). I have eleven years of software engineering experence with experience with message queues and trade compression debuggering by making a desktop app using Python and React I have a decade of professional experience in various industries such as insurance, CRM, Trade Show registration, recommender systems and cryptocurrency. I also have contributions to open source projects such as CPython documentation, triaging of issues and porting of features from Facebook's fork of Python.

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: PTP Flight Challenge
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Role play what would happen (or not happen) should a plane be maliciously targeted, or (like most) try and land a A320.

SpeakerBio: Pen Test Partners
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: PTP Flight Challenge
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Role play what would happen (or not happen) should a plane be maliciously targeted, or (like most) try and land a A320.

SpeakerBio: Pen Test Partners
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: PTP Flight Challenge
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Role play what would happen (or not happen) should a plane be maliciously targeted, or (like most) try and land a A320.

SpeakerBio: Pen Test Partners
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Friday - 16:00-18:59 PDT

Title: Pub Quiz
When: Friday, Aug 9, 16:00 - 18:59 PDT
Where: LVCC West/Floor 1/North Lobby/North Lobby Contests/ACK Stage - Map

Description:

We are back with another Pub Quiz at DEF CON. Here at Pub Quiz, we felt the need to add additional prizes for 4th and 5th place. We had a very successful one last year and we have made some improvements to make it every better. So do you like Pub Quizzes?? If you do then get your butts to join us in participating in the 2nd Pub Quiz at DEF CON 32.

Quiz will consist of 7 rounds question will include 90's/2000's TV and Movies, DefCon trivia, music, anime, and a little sex. The theme for our Pub Quiz will be all things that make DEF CON attendees exceptional. There will be a little something for everyone. The quiz will consist of visual and audio rounds along with some Con questions; we need to make sure we stimulate you peeps. We encourage people to get into teams of 5 or 6.

This is a social event, so we try to get people into Teams. You never know you may meet the love of your life. Did I mention CASH! Yes we will have cold hard cash prizes for the 1st, 2nd, 3rd, 4th, and 5th high scoring groups. As always if we do have ties will be break those ties with a good old fashion dance off from a person of the tied teams. The hosts and a few goons will help in judging.

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 17:05-17:45 PDT

Title: Pushing the limits of mass DNS scanning
When: Friday, Aug 9, 17:05 - 17:45 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Most hackers have a complicated, love-hate relationship with DNS: teleporting a fundamental building block of the internet from the 80's without major overhauls is a recipe for some interesting exploits and frustrations.

DNS enumeration is a critical process in penetration testing and essential to security practitioners: the faster we can conduct DNS enumeration, the more potential vulnerabilities we can find.

We developed an ultra-fast open-source DNS scanner, SanicDNS, using multiple parallelisation techniques. The result is a scanner that is two orders of magnitude faster than other popular tools. I will take attendees under the hood of the code, sharing what techniques yield the best results, the challenges encountered and their workarounds, and my tips for those considering the same endeavour.

The practical applications of SanicDNS far exceed those of everything that preceded it. With this novel scanner, it is possible to identify DNS misconfigurations and conduct Nameserver takeover scans across the entire internet in realtime. This opens up a world of new possibilities for conducting reconnaissance.

SanicDNS will be released for open-source at Defcon with easy-to-use installation instructions for the community.

SpeakerBio: Jasper Insinger

Jasper Insinger is a security researcher with a background in Electrical Engineering with a passion for low level / embedded computing. Before transitioning into security, Jasper worked on engineering the world's most efficient solar powered cars.

Return to Index - Add to Google - ics Calendar file

XRV - Friday - 10:00-10:59 PDT

Title: Pwning through the Metaverse - Quest Headset Vulnerability Research
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

This talk covers how to approach vulnerability research against Meta Quest headsets and VR applications.

We explore how to approach discovering bugs in the Meta Quest through the third-party app attack surface. This emulates what potentially malicious apps could achieve once installed and the unique attacks available in comparison to general mobile malware. This research culminates in a demonstration of triggering a novel vulnerability discovered in the OpenXR client implementation of the Quest.

Beyond this, we cover the unique remote attack surface exposed via the Horizons and first-party social app of the Quest - in particular we focus on attacking the rendering of user avatars. These bugs are possible to be triggered whenever within the same virtual space as a malicious user and represent a new attack surface not previously available. This research culminates in triggering a novel vulnerability in libovravatar2p.so which allows remote memory corruption and represents the building blocks for RCE across the metaverse.

SpeakerBio: Luke McLaren, Founder at Signal 11 Research Ltd

Luke McLaren is the founder of Signal 11 Research Ltd., a cybersecurity company specializing in mobile security research and training. With an impressive track record, Luke has claimed bug bounties from tech giants like Amazon, Meta, and Match.com. His expertise extends to virtual reality security, particularly with the Quest device series which he has worked with Meta to secure.

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Python + Packet Analysis + Machine Learning
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Use machine learning with Python to detect attacks in network packets including DNS tunneling, FTP brute force, and HTTP scanning. We will be using various Python tools such as iPython notebooks, scapy, and scikit-learn. Some Python experience is recommended, but if you don't know Python, come prepared to start with our Python tutorial!

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Python + Packet Analysis + Machine Learning
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Use machine learning with Python to detect attacks in network packets including DNS tunneling, FTP brute force, and HTTP scanning. We will be using various Python tools such as iPython notebooks, scapy, and scikit-learn. Some Python experience is recommended, but if you don't know Python, come prepared to start with our Python tutorial!

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Python + Packet Analysis + Machine Learning
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Use machine learning with Python to detect attacks in network packets including DNS tunneling, FTP brute force, and HTTP scanning. We will be using various Python tools such as iPython notebooks, scapy, and scikit-learn. Some Python experience is recommended, but if you don't know Python, come prepared to start with our Python tutorial!

Return to Index - Add to Google - ics Calendar file

APV - Friday - 13:00-14:59 PDT

Title: Q&A With OWASP
When: Friday, Aug 9, 13:00 - 14:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Pod 2 - Map

Description:

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 14:00-14:45 PDT

Title: QML - Quantum Machine Learning: What is it, where did it come from, and how do I start?
When: Saturday, Aug 10, 14:00 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Quantum machine learning is a relatively new discipline, first appearing around 15 years ago, and uses a combination of machine learning ideas and concepts with quantum computing in order to ask: can we utilize the high-dimensional vector space of quantum computing for machine learning?

In this talk, I'll go through the history of quantum machine learning: the highs, the lows, and the question marks. While we still have a lot to figure out — quantum computers will not just make existing quantum machine learning 'faster'! — I'll show you what's already out there and how to take part.

SpeakerBio: Josh Izaac

No BIO available

Return to Index - Add to Google - ics Calendar file

QTV - Sunday - 13:15-14:14 PDT

Title: QOLOSSUS CONTEST Q-CTF Finals
When: Sunday, Aug 11, 13:15 - 14:14 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 10:00-10:59 PDT

Title: QOLOSSUS: QUANTUM CTF CONTEST: How to get Started on The Quantum Capture The Flag
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: QOLOSSUS
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

There’s a new emerging tech in town, and it’s name is Quantum! Following the past two years of Quantum CTF events held at the Quantum Village, we are pleased, proud, and excited to announce that our Q-CTF is indeed returning as Codename; QOLOSSUS! Pit your wits against the Atom, and come and see what devilish challenges from our Quantum Quizmasters await. Come and show your quantum prowess, and mastery of superposition and entanglement - design algorithms to break cryptography, hack our simulated quantum communications, and score points in our IRL activities. |Good Luck!·

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: QOLOSSUS
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

There’s a new emerging tech in town, and it’s name is Quantum! Following the past two years of Quantum CTF events held at the Quantum Village, we are pleased, proud, and excited to announce that our Q-CTF is indeed returning as Codename; QOLOSSUS! Pit your wits against the Atom, and come and see what devilish challenges from our Quantum Quizmasters await. Come and show your quantum prowess, and mastery of superposition and entanglement - design algorithms to break cryptography, hack our simulated quantum communications, and score points in our IRL activities. |Good Luck!·

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: QOLOSSUS
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

There's a new emerging tech in town, and it's name is Quantum! Following the past two years of Quantum CTF events held at the Quantum Village, we are pleased, proud, and excited to announce that our Q-CTF is indeed returning as Codename; QOLOSSUS! Pit your wits against the Atom, and come and see what devilish challenges from our Quantum Quizmasters await. Come and show your quantum prowess, and mastery of superposition and entanglement - design algorithms to break cryptography, hack our simulated quantum communications, and score points in our IRL activities. |Good Luck!·

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 17:00-17:59 PDT

Title: Quantum Leap: The future of Computing and the security of your online world
When: Saturday, Aug 10, 17:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Join us for a journey into the world of quantum computing, where quantum computers can solve problems in seconds that would take regular computers years to solve. We'll explore the principles of quantum mechanics that make this possible, and the implications for cybersecurity. But don't worry, we'll also cover what's being done to keep our online communications safe and how we can stay ahead of the game.

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 14:00-14:59 PDT

Title: Quantum on the flip side - A global south perspective on Quantum Technologies
When: Friday, Aug 9, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

In this talk Bruna will bring to the table societal aspects of quantum technologies from a Global South perspective. In particular, how different are the dynamics of quantum hype in non-English speaking countries, how economic inequality affects quantum-readiness and why this should be everyone's problem.

SpeakerBio: Bruna Shinohara de Mendonça

Bruna Shinohara is a Staff Scientist specialized in Quantum Technologies from Brazil, currently working at CMC Microsystems, Canada. She holds a PhD in Physics, focusing on Condensed Matter Theory and Quantum Computation. She is also engaged in science outreach and advocates for democratizing access to information.

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 16:30-17:59 PDT

Title: Quantum Village Bloch Party!
When: Saturday, Aug 10, 16:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Join us for our first Bloch Party and find out anything you have wanted to know about Quantum Tech & Hacking and why it's a Bloch Party, not Block Party. At the same time join us for another round of our Oxford Union-style fun debates @ DEF CON!

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 16:00-17:59 PDT

Title: QueerCon Mixer
When: Saturday, Aug 10, 16:00 - 17:59 PDT
Where: LVCC West/Floor 2/W231-W233 - Map

Description:

Come by this informal mixer to meet others in the lgbtqia+ community who are a part of this wonderful world that is InfoSec. This is a safe and inclusive space to meet and talk to others with your shared experience and is a nice environment to network and unwind with a drink.

Return to Index - Add to Google - ics Calendar file

SOC - Thursday - 16:00-17:59 PDT

Title: QueerCon Mixer
When: Thursday, Aug 8, 16:00 - 17:59 PDT
Where: LVCC West/Floor 2/W231-W233 - Map

Description:

Come by this informal mixer to meet others in the lgbtqia+ community who are a part of this wonderful world that is InfoSec. This is a safe and inclusive space to meet and talk to others with your shared experience and is a nice environment to network and unwind with a drink.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 16:00-17:59 PDT

Title: QueerCon Mixer
When: Friday, Aug 9, 16:00 - 17:59 PDT
Where: LVCC West/Floor 2/W231-W233 - Map

Description:

Come by this informal mixer to meet others in the lgbtqia+ community who are a part of this wonderful world that is InfoSec. This is a safe and inclusive space to meet and talk to others with your shared experience and is a nice environment to network and unwind with a drink.

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 22:00-00:59 PDT

Title: QueerCon
When: Friday, Aug 9, 22:00 - 00:59 PDT
Where: LVCC West/Floor 3/W325-W326 - Map

Description:

A fun gathering space for the lgbtqia+ community to listen to DJ dance music and party together. An inclusive and vibrant option with others in the community.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 11:30-12:15 PDT

Title: QuickShell: Sharing is caring about an RCE attack chain on Quick Share
When: Saturday, Aug 10, 11:30 - 12:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

Quick Share (formerly Nearby Share) has enabled file sharing on Android for 4 years and expanded to Windows a year ago.

Google's promotion of Quick Share for preinstallation on Windows, alongside the limited recent research, ignited our curiosity about its safety, leading to an investigation that uncovered more than we had imagined.

We studied its Protobuf-based protocol using hooks, built tools to communicate with Quick Share devices, and a fuzzer that found non-exploitable crashes in the Windows app. We then diverted to search for logical vulnerabilities, and boy oh boy, we regretted we hadn't done it sooner.

We found 10 vulnerabilities both in Windows & Android allowing us to remotely write files into devices without approval, force the Windows app to crash in additional ways, redirect its traffic to our WiFi AP, traverse paths to the user's folder, and more. However, we desired the holy grail, an RCE. Thus, we returned to the drawing board, where we realized that the RCE is already in our possession in a form of a complex chain.

In this talk, we'll introduce QuickShell - An RCE attack chain on Windows combining 5 out of 10 vulnerabilities in Quick Share. We'll provide an overview about Quick Share's protocol, present our fuzzer, the found vulnerabilities, a new HTTPS MITM technique, and finally the RCE chain.

Reference link

Speakers: Or Yair,Shmuel Cohen

SpeakerBio: Or Yair, Security Research Team Lead at SafeBreach

Or Yair is a security research professional with six years of experience, currently serving as the Security Research Team Lead at SafeBreach. His primary focus lies in vulnerabilities in the Windows operating system's components, though his past work also included research of Linux kernel components and some Android components. Or has already presented his vulnerability and security research discoveries internationally at conferences he spoke at such as Black Hat USA 2023, Black Hat Asia 2024, Black Hat Europe 2022, SecTor 2023, RSAC 2023, Security Fest 2023, CONFidence 2023 & 2024 and more

SpeakerBio: Shmuel Cohen, Senior Security Researcher at SafeBreach

Shmuel Cohen is a cybersecurity professional, who has a diverse background. After he pursued a Bachelor of Science degree in Computer Science, he had the privilege of working at CheckPoint, where he spent 1.5 years developing software and another 1.5 years working as a malware security researcher. As his interest grew in vulnerability research, he decided to join SafeBreach, where he has been able to focus his energies on exploring and addressing vulnerabilities in cybersecurity. Shmuel has previously spoken at BlackHat USA 2023, twice at Black Hat Asia 2024, and twice at CONFidence 2024.

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 21:00-01:59 PDT

Title: RAA for Workgroups 3.11
When: Saturday, Aug 10, 21:00 - 01:59 PDT
Where: LVCC West/Floor 3/W322-W324, W327 - Map

Description:

RAA For Workgroups 3.11 is a continuation of the Rent an Assassin series of parties from DC Shenanigans. Based on the World of Assassination from the Hitman video game franchise, RAA has been serving up clandestine client acquisition events in top-secret locations since DC30. This year marks our first-ever official DEF CON event, and we are excited to bring you some of the best DJs (and shenanigans) DEF CON has to offer.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Radio Frequency Capture the Flag
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and $0 to $$$$$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Radio Frequency Capture the Flag
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and $0 to $$$$$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: Radio Frequency Capture the Flag
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and $0 to $$$$$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-12:59 PDT

Title: Radio Frequency Capture the Flag
When: Friday, Aug 9, 10:00 - 12:59 PDT
Where: Virtual

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and $0 to $$$$$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 10:00-17:59 PDT

Title: Radio Frequency Village Events
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

In addition to the CTF and talks which are elsewhere on the schedule, the RF Village is also a place to hang out and chat with like minded folks who share your interests.

Return to Index - Add to Google - ics Calendar file

RFV - Sunday - 10:00-12:59 PDT

Title: Radio Frequency Village Events
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

In addition to the CTF and talks which are elsewhere on the schedule, the RF Village is also a place to hang out and chat with like minded folks who share your interests.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 10:00-17:59 PDT

Title: Radio Frequency Village Events
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

In addition to the CTF and talks which are elsewhere on the schedule, the RF Village is also a place to hang out and chat with like minded folks who share your interests.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 15:00-15:30 PDT

Title: Ransomware B-Sides: Los ransoms que nunca triunfaron
When: Saturday, Aug 10, 15:00 - 15:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

Este es un triple disco de vinilo. En el Lado A, abordaremos el panorama de los ransomwares, los famosos, por supuesto, y cómo los ransomware indies intentan competir con los ya consagrados. Al igual que en el lado B de un disco, se encuentran las canciones más oscuras y desconocidas que es poco probable que escuches por ahí, trataremos de los ransomwares que nunca han llegado al estrellato. Y por último, en LadoC, echaremos un vistazo a las amenazas emergentes y a las recomendaciones.

Speakers: Mauro Eldritch,Cybelle Oliveira

SpeakerBio: Mauro Eldritch, Founder at Birmingham Cyber Arms LTD

Mauro Eldritch is an Argentine hacker, founder of Birmingham Cyber Arms LTD and DC5411 (Argentina / Uruguay). He has spoken at various events, including DEF CON (10 times). He is passionate about Threat Intelligence and Biohacking.

Mauro Eldritch es un hacker argentino, fundador de Birmingham Cyber Arms LTD y DC5411 (Argentina / Uruguay). Habló en diferentes eventos incluyendo DEF CON (10 veces). Le apasiona la Inteligencia de Amenazas y el Biohacking.

SpeakerBio: Cybelle Oliveira , CTI Malwarelandia

Cybelle Oliveira is a Cybersecurity Consultant, postgraduate in Cyber Threat Intelligence and Master's student in Cyber intelligence at the International Cybersecurity Campus of the University of Murcia, Spain. She has been involved in privacy and security activism for over 10 years and has presented talks at events around the world, including BSides LV, BSides SP, Girls Hack Village (DefCon), 8.8 Chile, Internet Freedom Festival, Radical Networks, Mozilla Festival, Roadsec, Cryptorave, among others. Cybelle is part of the Mozilla community and is the director of the Casa Hacker organization.

Cybelle Oliveira es Consultora de Ciberseguridad, postgraduada en Cyber Threat Intelligence y estudiante de Máster en Ciberinteligencia en el Campus Internacional de Ciberseguridad de la Universidad de Murcia, España. Ha estado involucrada en activismo de privacidad y seguridad durante más de 10 años y ha presentado charlas en eventos por todo el mundo, como BSides LV, BSides SP, Girls Hack Village (DefCon), 8.8 Chile, Internet Freedom Festival, Radical Networks, Mozilla Festival, Roadsec, Cryptorave, entre otros. Cybelle forma parte de la comunidad Mozilla y es directora de la organización Casa Hacker.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 15:00-15:59 PDT

Title: Real life hacking stories (that can’t be recorded!)
When: Saturday, Aug 10, 15:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Panel - Hacker stories and career Q and A: Stories and adventures from real life hacking engagements. Ask the panel about different career’s in cyber security and getting paid to be a hacker.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: REALI7Y OVERRUN
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-E - Map

Description:

This is going to be an interactive live game that is driven by a near future storyline in which deepfakes and forgeries are so difficult to detect that bad actors and foreign governments are fully engaged in a war over people's minds. At the same time, the world is sitting on the brink of the so-called "singularity," as AI advancements have completely blurred the line between artificial and natural cognition, and the Turing test has been rendered decisively moot.

Teams will join the game and follow the storyline to clues that will give them hints about who they can trust and who they can't. The clues will follow the pattern of deepfakes and forgeries, asking players to figure out what's real and what's not, focusing on hacker and defcon focus areas such as authentication, trust, social engineering, hardware and software manipulation and more. They will be given a rich story that will lead them to research the underlying issues in trust and anonymous trust systems. They will also encounter challenges and tutorials on video and image validation and cryptographically safe messaging.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: REALI7Y OVERRUN
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-E - Map

Description:

This is going to be an interactive live game that is driven by a near future storyline in which deepfakes and forgeries are so difficult to detect that bad actors and foreign governments are fully engaged in a war over people's minds. At the same time, the world is sitting on the brink of the so-called "singularity," as AI advancements have completely blurred the line between artificial and natural cognition, and the Turing test has been rendered decisively moot.

Teams will join the game and follow the storyline to clues that will give them hints about who they can trust and who they can't. The clues will follow the pattern of deepfakes and forgeries, asking players to figure out what's real and what's not, focusing on hacker and defcon focus areas such as authentication, trust, social engineering, hardware and software manipulation and more. They will be given a rich story that will lead them to research the underlying issues in trust and anonymous trust systems. They will also encounter challenges and tutorials on video and image validation and cryptographically safe messaging.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: REALI7Y OVERRUN
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-E - Map

Description:

This is going to be an interactive live game that is driven by a near future storyline in which deepfakes and forgeries are so difficult to detect that bad actors and foreign governments are fully engaged in a war over people's minds. At the same time, the world is sitting on the brink of the so-called "singularity," as AI advancements have completely blurred the line between artificial and natural cognition, and the Turing test has been rendered decisively moot.

Teams will join the game and follow the storyline to clues that will give them hints about who they can trust and who they can't. The clues will follow the pattern of deepfakes and forgeries, asking players to figure out what's real and what's not, focusing on hacker and defcon focus areas such as authentication, trust, social engineering, hardware and software manipulation and more. They will be given a rich story that will lead them to research the underlying issues in trust and anonymous trust systems. They will also encounter challenges and tutorials on video and image validation and cryptographically safe messaging.

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 15:45-16:20 PDT

Title: Recon MindMap: Organize, Visualize, and Prioritize Your Recon Data Efficiently
When: Friday, Aug 9, 15:45 - 16:20 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

After doing recon on a target you probably end up with more URLs, domains and IPs that you can handle, and when time is limited, how do you prioritize them? Recon MindMap (RMM) is a tool that will simplify the task of organizing and sorting all these assets. RMM can help you to generate complex domain structures, visualize them using your favorite mind map tools, make informed decisions, and improve your reports visual appeal.

During the talk I'll discuss the motivations behind building this tool and what problem it solves, the algorithm behind, scenarios and use cases for this tool, how to contribute to the project and what's next for RMM.

RMM it's opensource and it's available at https://github.com/Alevsk/rmm

SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 10:00-13:59 PDT

Title: Recon Village GE(O)SINT Challenge
When: Friday, Aug 9, 10:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Join the Recon Village GEOSINT Challenge, where your geospatial intelligence skills will be put to the ultimate test. Navigate through complex scenarios, uncover hidden clues, and outsmart your competition. Sharpen your analytical prowess and prove your mastery in this thrilling contest of wits and strategy.

Return to Index - Add to Google - ics Calendar file

RCV - Saturday - 10:00-13:59 PDT

Title: Recon Village GE(O)SINT Challenge
When: Saturday, Aug 10, 10:00 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Join the Recon Village GEOSINT Challenge, where your geospatial intelligence skills will be put to the ultimate test. Navigate through complex scenarios, uncover hidden clues, and outsmart your competition. Sharpen your analytical prowess and prove your mastery in this thrilling contest of wits and strategy.

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 10:45-11:30 PDT

Title: Recursion is a Harsh Mistress: How (Not) To Build a Recursive Internet Scanner
When: Friday, Aug 9, 10:45 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Recursion has a tendency to turn little bugs into explosive ones. In this talk, witness the myriad of strange and unexpected bugs we encountered while building BBOT, a recursive internet scanner. Rendered in smooth realtime animations, these bugs may appear fun and sometimes hilarious, but when they occurred they were extremely problematic, and taught us some valuable lessons about the internet and recursion.

Discover the nefarious traps and nightmarish edge cases that awaited us in the depths of the internet, the destruction they caused, the awkward situations they put us in, and the tricks we used to overcome them. Most importantly, discover the kinds of hidden gems recursion can uncover (when it's implemented properly), and the critical advantage it will give you in your recon!

SpeakerBio: TheTechromancer
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-16:59 PDT

Title: Red Alert ICS CTF
When: Saturday, Aug 10, 10:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-07 - Map

Description:

Red Alert ICS CTF is a competition for Hackers by Hackers, organized by the RedAlert Lab of NSHC Security. The event exclusively focuses on having the participants clear a series of challenges and break through several layers of security in our OT environment and eventually take over complete control of the ICS components.

Red Alert ICS CTF is back with a ton of fun challenges after successfully running the CTF since DEF CON 26. Red Alert ICS CTF is proud to be among the Black Badge contests at DEF CON 31 and DEF CON 26.

The contest would house real world ICS (Industrial Control System) equipment from various vendors on showcasing different sectors of critical infrastructure. The participants would be able to view and engage with the devices in real time and understand how each of them control each of the aspects of the testbed and leverage this to compromise the devices.

Red Alert ICS CTF at DEF CON 32 would also be offering players the unique opportunity to compromise the latest cyber ranges on Maritime Cyber Security.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 12:00-16:59 PDT

Title: Red Alert ICS CTF
When: Friday, Aug 9, 12:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-07 - Map

Description:

Red Alert ICS CTF is a competition for Hackers by Hackers, organized by the RedAlert Lab of NSHC Security. The event exclusively focuses on having the participants clear a series of challenges and break through several layers of security in our OT environment and eventually take over complete control of the ICS components.

Red Alert ICS CTF is back with a ton of fun challenges after successfully running the CTF since DEF CON 26. Red Alert ICS CTF is proud to be among the Black Badge contests at DEF CON 31 and DEF CON 26.

The contest would house real world ICS (Industrial Control System) equipment from various vendors on showcasing different sectors of critical infrastructure. The participants would be able to view and engage with the devices in real time and understand how each of them control each of the aspects of the testbed and leverage this to compromise the devices.

Red Alert ICS CTF at DEF CON 32 would also be offering players the unique opportunity to compromise the latest cyber ranges on Maritime Cyber Security.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 13:00-13:50 PDT

Title: Red Goes Purple: Executing the Attack Path
When: Friday, Aug 9, 13:00 - 13:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

In this collaborative panel with Blue Team Village we'll sit down with two Red Teamers and two Blue Teamers to talk through how real world attacks could take place - and how to defend them.

Speakers: Omar Santos,Graham Helton,Kevin "Kent" Clark

SpeakerBio: Omar Santos
No BIO available
SpeakerBio: Graham Helton
No BIO available
SpeakerBio: Kevin "Kent" Clark, Security Consultant at TrustedSec

Kevin "Kent" Clark is a Security Consultant with TrustedSec and a Red Team Instructor with BC Security. His previous work includes Penetration Testing and Red Team Operator, focusing on initial access and active directory exploitation. Kevin contributes to open-source tools such as PowerShell Empire and publishes custom security toolkits such as Badrats and WindowsBinaryReplacements. Kevin authors a cybersecurity blog at https://henpeebin.com/kevin/blog.

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 11:00-11:50 PDT

Title: Red Team Infrastructure Setup and Automation
When: Sunday, Aug 11, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

This workshop offers a fast-paced and engaging introduction to setting up Red Team Infrastructure, focusing on the practical use of Terraform and Ansible. The session begins with a brief overview of Red Team operations and the critical role of robust infrastructure. It then swiftly moves into the practical aspects, demonstrating the basics of Terraform for deploying cloud infrastructure and Ansible for efficient configuration management. The highlight is a demonstration on integrating these tools to automate key components of Red Team infrastructure, emphasizing their application in real-world scenarios. This workshop is tailored for those eager to quickly grasp the essentials of Red Team infrastructure automation.

Speakers: Aravind Prakash,Arun Nair,Shebin Mathew

SpeakerBio: Aravind Prakash
No BIO available
SpeakerBio: Arun Nair
No BIO available
SpeakerBio: Shebin Mathew
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 12:00-12:50 PDT

Title: Red Team Terraform Workshop
When: Friday, Aug 9, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

How to build automated Red Team Infrastructure that is composable and reproducable.

SpeakerBio: Moses Frost
No BIO available

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-16:59 PDT

Title: Red Team Village CTF
When: Friday, Aug 9, 10:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05-C - Map

Description:

The Red Team Capture the Flag (CTF) competition is back at DEFCON! It is a challenging and exciting event that tests the skills of participants in offensive security.

The Red Team CTF is designed to simulate real-world challenges in which attackers are put to the test. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities.

Teams are typically composed of experienced hackers, penetration testers, and security researchers who have a deep understanding of the latest cybersecurity threats and attack techniques. They must work together to uncover and exploit vulnerabilities and solve challenges.

The Red Team CTF at DEFCON is considered one of the most challenging and prestigious CTF competitions in the world, with participants coming from all over the globe to compete. It is a high-pressure, high-stakes event that tests the limits of participants' technical and strategic abilities, and offers a unique opportunity to showcase their skills and knowledge in front of a global audience of Hackers.

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Red Team Village CTF
When: Sunday, Aug 11, 10:00 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05-C - Map

Description:

The Red Team Capture the Flag (CTF) competition is back at DEFCON! It is a challenging and exciting event that tests the skills of participants in offensive security.

The Red Team CTF is designed to simulate real-world challenges in which attackers are put to the test. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities.

Teams are typically composed of experienced hackers, penetration testers, and security researchers who have a deep understanding of the latest cybersecurity threats and attack techniques. They must work together to uncover and exploit vulnerabilities and solve challenges.

The Red Team CTF at DEFCON is considered one of the most challenging and prestigious CTF competitions in the world, with participants coming from all over the globe to compete. It is a high-pressure, high-stakes event that tests the limits of participants' technical and strategic abilities, and offers a unique opportunity to showcase their skills and knowledge in front of a global audience of Hackers.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-16:59 PDT

Title: Red Team Village CTF
When: Saturday, Aug 10, 10:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-05-C - Map

Description:

The Red Team Capture the Flag (CTF) competition is back at DEFCON! It is a challenging and exciting event that tests the skills of participants in offensive security.

The Red Team CTF is designed to simulate real-world challenges in which attackers are put to the test. Participants are expected to use a wide range of hacking techniques, tools, and skills to identify and exploit vulnerabilities.

Teams are typically composed of experienced hackers, penetration testers, and security researchers who have a deep understanding of the latest cybersecurity threats and attack techniques. They must work together to uncover and exploit vulnerabilities and solve challenges.

The Red Team CTF at DEFCON is considered one of the most challenging and prestigious CTF competitions in the world, with participants coming from all over the globe to compete. It is a high-pressure, high-stakes event that tests the limits of participants' technical and strategic abilities, and offers a unique opportunity to showcase their skills and knowledge in front of a global audience of Hackers.

Return to Index - Add to Google - ics Calendar file

ADV - Friday - 17:00-17:59 PDT

Title: Red Teaming is broken; this panel will fix it.
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:
Speakers: Suneel Sundar,Niru Ragupathy,Joe Vest,Drinor Selmanaj

SpeakerBio: Suneel Sundar, Director of Research & Development, Center for Threat-Informed Defense
No BIO available
SpeakerBio: Niru Ragupathy, Security Engineer - Manager at Google

Niru is a security engineer - manager at Google. She leads the Offensive security team, where she supports the program and works on red team exercises. In her free time she doodles corgis and writes CTF challenges.

SpeakerBio: Joe Vest, Author of Red Team Development and Operations

Driven by his curiosity, perseverance, and passion for technology, Joe Vest's mantra for his work and teaching is: "The journey of gaining experience can be as valuable as the end result." Joe has over 20 years of experience in technology with a focus on red teaming, When Joe is not working, you can find him enjoying life in the sun on the coast of Florida.penetration testing, and application security. Joe is currently a Principal Security Engineer at AWS. Prior experience includes the Cobalt Strike Technical Director at HelpSystems, a security consulting company entrepreneur and owner, and a former director at SpecterOps. This diverse experience has given him extensive knowledge of cyber threats, tools, and tactics, including threat emulation and threat detection. Notable career accomplishments include authoring the book "Red Team Development and Operations" and authoring the original SANS 564 red team course.

SpeakerBio: Drinor Selmanaj, Founder of Sentry Cybersecurity and Defense
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 12:30-13:15 PDT

Title: Redefining V2G - How to use your vehicle as a game controller
When: Sunday, Aug 11, 12:30 - 13:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Modern cars are a complex networks of computers put on four wheels. For security research, it is important to understand the car's internal network and exposed interfaces. But what else could you use this knowledge for? You probably guessed it from the title . So we developed a tool to turn our research car into a game controller.

In this talk, we present Vehicle-to-Game (V2G), a Python-based project that enables the usage of cars as game controllers. V2G can run either directly on a laptop or turn a Raspberry Pi Zero WH into a Bluetooth gamepad. In addition, V2G can either be used over the OBD2-diagnostic port or by directly accessing the internal CAN-busses of the car.

Our project can be a great starting point if you always wanted to tinker around with your car or want to learn about the CAN bus or diagnostic communication (UDS). To make V2G work with your car, some reverse engineering of CAN messages or diagnostic communication will be required (as well as additional hardware to connect to the CAN bus). Otherwise, if you can get this running, you can be sure that you own a more expensive game controller than your neighbors.

Tools and hardware: 1. General introduction into the CAN-bus and UDS: link 2. Tool for designing PCBs: link 3. Tool for making CAN messages readable: link 4. Hardware for accessing CAN-bus and OBD: link 5. CAN utils: link 6. CAN hat for Raspberry Pi: link

Used libraries: 1. link Many thanks for providing this great library and documentation for utilizing the Raspberry Pi as a Bluetooth device! 2. link 3. link

Misc: 1. Tesla DBC files: link 2. ACSD website: link 3. V2G Repository on GitHub (private until start of DEF CON): link

Speakers: Timm Lauser,Jannis Hamborg

SpeakerBio: Timm Lauser, PhD Student at Darmstadt University of Applied Sciences

Timm Lauser received his masters degree in computers science from Karlsruhe Institute of Technology, Germany in 2020. Since then, he is a PhD student at Darmstadt University of Applied Sciences, Germany. There, he is researching in the field of automotive cyber security with a focus on communication protocols and their formal verification in the symbolic model.

SpeakerBio: Jannis Hamborg, PhD Student at Darmstadt University of Applied Sciences

Jannis Hamborg received his masters degree in computer science with focus on IT-security from Technical University Darmstadt, Germany in 2023. For his master thesis he researched about resilient and self-recovering reputation based networks. During the time of master he worked as assistant researcher at Darmstadt University of Applied Sciences, Germany on different topics of automotive security research. Since end of 2023, he started his PhD on the design and integration of resilient risk-driven networks with focus on internal automotive networks.

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 17:00-17:59 PDT

Title: Reflections on a Decade in Bug Bounties: Experiences and Major Takeaways
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

In this talk, I will share my journey from a novice to a seasoned hunter. I will explore how I used to report low-impact, informative bugs when I first started, and how I progressively improved by learning from the community, embracing failures/duplicates, and incorporating feedback from triage teams and clients. This journey of continuous learning and adaptation led me from reporting low vulnerabilities to effectively chaining and converting them into critical impacts.

This session is designed for both aspiring and experienced bug bounty hunters. By reflecting on a decade of lessons learned, I will aim to provide valuable takeaways that can help others navigate their own paths in bug bounty hunting and enhance their skills.

Additionally, one Synack triage team member will join me on this talk to help differentiate triage thinking from bug bounty hunters' thinking, providing valuable insights into the collaborative process of vulnerability reporting to acceptance.

Speakers: Charles Waterhouse,Nikhil "niks" Shrivastava

SpeakerBio: Charles Waterhouse

After spending over 2 decades in the airline industry, I changed careers into cybersecurity. I have helped manage over 2400 engagements with teams of over 1000 researchers across all verticals in commercialand government. I regularly consult with executives in many Global 500 organizations and government to developsecurity and testing plans.

I have helped develop products around OWASP, NIST, OSINT, API and AI testing. I speak regularly at conferences and help train developers and blue teams to help defend some of the most critical networks worldwide.

SpeakerBio: Nikhil "niks" Shrivastava

My Name is Nikhil Shrivastava AKA niksthehacker. I am an ethical hacker and bug bounty hunter. I have helped over 300 companies to uncover 1500+ Security Vulnerabilities such as Google, Microsoft, Tesla, Mozilla, Salesforce, eBay, Federal Agencies, and many more. I am the #1 hacker in India at Synack Red Team. I was awarded "Synack Legend Hacker" Status in 2021. I have also been interviewed by Defcon Red Team Village, Synack, and Indian media such as the Times of India, Economic Times, Indian Express, etc. I was also MSRC (Microsoft Security Response Center) Top 100 Hackers in 2016. I am the founder of Security BSides Ahmedabad, an international hacking conference hosted each year in Ahmedabad, India.

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-17:59 PDT

Title: Regular Expressions (RegEx) Trainer
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Regular Expressions or RegEX are used everywhere! If you aspire to be a Pentester, Threat Hunter, Programmer, Network Engineer, DevOps or really anything in technology today, RegEx is a skill all the greats have and the majority of the industry are terrible at. Come learn or brush up on your RegEx skills in on our live trainer.

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 10:00-13:59 PDT

Title: Regular Expressions (RegEx) Trainer
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Regular Expressions or RegEX are used everywhere! If you aspire to be a Pentester, Threat Hunter, Programmer, Network Engineer, DevOps or really anything in technology today, RegEx is a skill all the greats have and the majority of the industry are terrible at. Come learn or brush up on your RegEx skills in on our live trainer.

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 10:00-17:59 PDT

Title: Regular Expressions (RegEx) Trainer
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 2/W216-W221 - Map

Description:

Regular Expressions or RegEX are used everywhere! If you aspire to be a Pentester, Threat Hunter, Programmer, Network Engineer, DevOps or really anything in technology today, RegEx is a skill all the greats have and the majority of the industry are terrible at. Come learn or brush up on your RegEx skills in on our live trainer.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 14:00-14:30 PDT

Title: Relative Path File Injection: The Next Evolution in RPO
When: Friday, Aug 9, 14:00 - 14:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Most web security professionals are familiar with Relative Path Overwrite (RPO) attacks that allow injecting malicious CSS via a quirk in how browsers handle paths. But what if you could use a similar technique to get victims to download malicious files by clicking an innocuous looking download link on a trusted site? In this presentation, we'll unveil a new attack vector dubbed Relative Path File Injection (RPFI) that abuses path handling to turn benign websites into malware delivery platforms. Attendees will learn the anatomy of an RPFI attack, see demos of it in action, and learn how to detect this overlooked vulnerability class in the wild. We'll also release an open source GitHub repo with proof of concepts for users to try for themselves. RPFI represents a new breed of polyglot-based attack that exploits gaps between web specifications and real-world implementations.

SpeakerBio: Ian Hickey

Ian Hickey, is a software developer in the Edtech space and devotes some time each week trying to solve problems that have not been solved before. His professional journey has been a unique blend of coding and education. As a software developer, he delved deep into the intricacies of how technology can enhance learning experiences. He mostly dabbles in security as a hobby. I am a lifelong hacker and I'm an active member of HackerOne and similar bug bounty programs.

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 14:00-14:59 PDT

Title: Remote Sensor Node Updates for FISSURE - The RF Framework
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

New updates to FISSURE, the open-source RF framework and toolbox for all things RF, include the addition of deployable remote sensor nodes consisting of general-purpose computers that support many types of radio peripherals. These remote sensor nodes run a small subset of code that can be controlled over a network through the FISSURE Dashboard GUI to perform traditional FISSURE operations and also execute new types of scripted actions that can be run autonomously on startup or semi-autonomously through user interaction.

Flexible hardware options inherent to the computers and the radio peripherals allow the operator to weigh varying price points and upgrade options depending on the task at hand. Multiple types of COTS single-board computers (Raspberry Pi, Orange Pi, etc.), mini-PCs, laptops, and desktop computers can be supported along with various RF-enabled devices like software-defined radios or Wi-Fi/Bluetooth/Zigbee adapters. The new updates also include the ability to trigger electromagnetic effects using different types of RF, visual, acoustic, and environmental sensors connected to the nodes.

The deployment of multiple sensor nodes on the same network unlocks many geospatial applications for future development of FISSURE. Such applications include direction finding, tracking, intrusion detection, mobile deployment, and perimeter defense. A small form factor and autonomous capabilities grant unique opportunities for stealth deployment and packaging onto existing platforms. These updates can also provide a low-cost mechanism for remote workers to conduct combined RF-cybersecurity testing and access specialized RF environments like international localities of interest, laboratories, and test sites.

This talk will provide a brief overview of FISSURE and walk through all the new updates relating to the remote sensor node capabilities. To learn more, read about FISSURE on GitHub: https://github.com/ainfosec/FISSURE

SpeakerBio: Chris Poore, Senior Reverse Engineer at Assured Information Security

Chris Poore is a Senior Reverse Engineer at Assured Information Security in Rome, NY and is the lead developer for FISSURE. He has expertise discovering vulnerabilities in wireless systems, gaining access to systems via RF, reverse engineering RF protocols, forensically testing cybersecurity systems, and administering RF collection events.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 15:00-15:59 PDT

Title: Removing OPSEC from Cyber Predators and Threat Actors
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

One of the major problems faced by law enforcement and investigators is the process of identifying threat actors who use the tor network. The purpose of this work is to show that sometimes these Threat Actors fall into the same problems as other victims of malicious artifacts on the Internet.

SpeakerBio: Thiago Bordini, Head Cyber Threat Intelligence

Thiago Bordini, Head Cyber Threat Intelligence, executive with more than 20 years of experience in the cyber intelligence market, working with analysis and prevention of cyber threats and fraud and dissemination of educational content on the subject to professionals and companies. Technical coordinator and postgraduate professor at IDESP.

Speaker at several national and international events such as YSTS, EkoParty,

H2HC, Security BSides, SANS, HTCIA, CoronaCon, 8.8 Andina and Brazil, among others.

Member of the HTCIA (High Technology Crime Investigation Association).

Member of the Security BSides Sao Paulo/Brazil organization.

Return to Index - Add to Google - ics Calendar file

AIV - Friday - 14:30-14:59 PDT

Title: Removing the Ring of Gyges: Lessons from Securing AI Systems Against File Format Abuse
When: Friday, Aug 9, 14:30 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

This talk will focus on the implications of our work defending AI based cybersecurity systems against file format abuse for the design of AI systems for cyber. The audience will learn how the interface between traditional cybersecurity systems and the AI models being integrated into them impacts security. File format abuse enables polyglot files to bypass state-of-the-art malware detection systems (EDR tools) that utilize machine learning in an attempt to catch novel forms of malware. The polyglot file is sent to the wrong model because the embedded file type is not detected. Existing file type, file carving, and polyglot detection tools are insufficient to detect polyglots used by threat actors in the wild. However, we trained a machine learning model capable of detecting all polyglot types in our dataset, which is based on threat actor usage of polyglots in the wild, with over 99.9% accuracy. Content disarm and reconstruct (CDR) tools can also be used to disarm polyglots, but are not effective on all file types.

Speakers: Sean Oesch,Luke Koch,Brian Weber,Amul Chaulagain,Matthew Dixson,Jared Dixon,Cory Watson

SpeakerBio: Sean Oesch, Oak Ridge National Laboratory
No BIO available
SpeakerBio: Luke Koch, Oak Ridge National Laboratory
No BIO available
SpeakerBio: Brian Weber, Oak Ridge National Laboratory
No BIO available
SpeakerBio: Amul Chaulagain, Oak Ridge National Laboratory
No BIO available
SpeakerBio: Matthew Dixson
No BIO available
SpeakerBio: Jared Dixon
No BIO available
SpeakerBio: Cory Watson
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-12:59 PDT

Title: Resume Reviews
When: Saturday, Aug 10, 10:00 - 12:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Resume Reviews offer attendees the opportunity to have their resumes critiqued by industry professionals. This activity provides personalized feedback and tips on how to improve resumes to stand out in the cybersecurity job market. It's a great way for participants to enhance their professional profiles and increase their chances of landing their desired roles.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-12:59 PDT

Title: Resume Reviews
When: Friday, Aug 9, 10:00 - 12:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Resume Reviews offer attendees the opportunity to have their resumes critiqued by industry professionals. This activity provides personalized feedback and tips on how to improve resumes to stand out in the cybersecurity job market. It's a great way for participants to enhance their professional profiles and increase their chances of landing their desired roles.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 14:00-17:59 PDT

Title: Resume Reviews
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Resume Reviews offer attendees the opportunity to have their resumes critiqued by industry professionals. This activity provides personalized feedback and tips on how to improve resumes to stand out in the cybersecurity job market. It's a great way for participants to enhance their professional profiles and increase their chances of landing their desired roles.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 14:00-17:59 PDT

Title: Resume Reviews
When: Saturday, Aug 10, 14:00 - 17:59 PDT
Where: LVCC West/Floor 2/W208 - Map

Description:

Resume Reviews offer attendees the opportunity to have their resumes critiqued by industry professionals. This activity provides personalized feedback and tips on how to improve resumes to stand out in the cybersecurity job market. It's a great way for participants to enhance their professional profiles and increase their chances of landing their desired roles.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-15:59 PDT

Title: Retro Repair
When: Saturday, Aug 10, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Although not scheduled we intend to have people in and out who can do repairs/soldering on older equipment should anything need it. If you have trouble with your vintage tech during con, we will do our best to help!

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-15:59 PDT

Title: Retro Repair
When: Friday, Aug 9, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Although not scheduled we intend to have people in and out who can do repairs/soldering on older equipment should anything need it. If you have trouble with your vintage tech during con, we will do our best to help!

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Retro Repair
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Although not scheduled we intend to have people in and out who can do repairs/soldering on older equipment should anything need it. If you have trouble with your vintage tech during con, we will do our best to help!

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 12:40-13:10 PDT

Title: Revealing Choke Points: Practical Tactics for Boosting Cloud Security
When: Saturday, Aug 10, 12:40 - 13:10 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

During this presentation, we will address the critical importance of permission management in Cloud Native integrations and how an inadequate permissions model can create significant advantages for attackers. We will demonstrate how an attacker can exploit standard permissions to achieve privilege escalation, explain what Choke Points are, and illustrate Attack Paths in practice, showing how an attacker can progress towards success in their objectives. As the ultimate goal of this talk, we will present practical actions to enhance the security of your environment in this context and mitigate these threats.

SpeakerBio: Filipi Pires, Founder at Black&White Technology

I’ve been working as Security and Threat Researcher and Cybersecurity Advocate at senhasegura, Founder at Black&White Technology, Cybersecurity Advocate, Snyk Ambassador, Application Security Specialist and Hacking is NOT a crime Advocate. International Speaker at Security and New technologies events in many countries such as US, Canada, France, Spain, Germany, Poland, and others, I’ve served as University Professor in Graduation and MBA courses at Brazilian colleges, in addition, I'm Creator and Instructor of the Course - Malware Attack Types with Kill Chain Methodology (PentestMagazine), PowerShell and Windows for Red Teamers(PentestMagazine) and Malware Analysis - Fundamentals (HackerSec).

Return to Index - Add to Google - ics Calendar file

ESV - Saturday - 15:15-15:59 PDT

Title: Reverse engineering and hacking Ecovacs robots
When: Saturday, Aug 10, 15:15 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Were you ever wondering why a vacuum robot or a smart air purifier needs multiple cameras and microphones? How secure are these devices? Can the devices be used to potentially spy on you?

For the past 5 years we have been presenting ways to hack and root vacuum robots at various events like the c3 or the DEFCON. In all these cases it covered vacuum robots by Roborock, Dreame, Xiaomi and some smaller companies. However, did we ever take a look at other vendors and maybe some new interesting device classes? In this talk we do exactly that, and will take a deep dive into Ecovacs robots! Ecovacs is the current market leader for smart home robots and recently expanded in other areas of home robotics.

You will be surprised how many worrisome things we found: broken crypto, missing TLS certificate verification, honor-system based ACLs, lots of RCEs, broken factory resets and unauthorized live camera access.

We will discuss our and other researchers experience with reporting bugs to the company and why one cannot trust third party certification agencies. In regard to trust, we will also address why you need to be careful with the choice of your spouse or flatmates.

Come with us on a journey of having fun hacking interesting devices while exploring bad oversights, real problems and the ignorance of the manufacturer. Learn what ways there are to root these devices and to use them in a privacy-preserving way.

Speakers: Dennis Giese,Braelynn

SpeakerBio: Dennis Giese

Dennis Giese is a researcher with the focus on the security and privacy of IoT devices. While being interested in physical security and lockpicking, he enjoys applied research and reverse engineering malware and all kinds of devices. His most known projects are the documentation and hacking of various vacuum robots. He calls himself a "robot collector" and his current vacuum robot army consists of over 60 different models from various vendors. He talked about his research at the Chaos Communication Congress, REcon BRX, NULLCON, and DEFCON.

SpeakerBio: Braelynn, Security Consultant at Leviathan Security Group

Braelynn is a security consultant at Leviathan Security Group where she conducts security assessments of products for startups, Fortune 500 companies, and everything in between. She enjoys partaking in CTFs and researching the security anything that piques her curiosity. She has previously presented this research at conferences such as Chaos Communication Congress.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 10:00-10:45 PDT

Title: Reverse Engineering MicroPython Frozen Modules: Data Structures, Reconstruction, and Reading Bytecode
When: Saturday, Aug 10, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

MicroPython is a firmware environment for quickly developing and deploying software onto microcontroller systems. It is used in a variety of industrial and scientific applications, as well as (most importantly) in some DEF CON #badgelife projects. It's easy to learn and use for rapid prototyping.

For hackers interested in reverse engineering compiled or obfuscated MicroPython code, there are some obstacles. MicroPython is an implementation of CPython, not a port, so it has its own compiled bytecode language that existing reverse engineering tools aren't designed to parse. Also, modules can be "frozen", compiled directly into the microcontroller firmware, and may be difficult to locate and parse when microcontroller firmware is extracted and analyzed.

In this talk, Wesley will walk the audience through the process of identifying "frozen"/compiled modules in a firmware image without debug symbols using the Ghidra disassembler. The relevant module, string, object, and raw code data structures will be detailed, so that everything required to rebuild a non-frozen module can recovered. Once a compiled module is reconstructed, Wesley will present a detailed example of reading and understanding MicroPython compiled bytecode, for the purpose of reverse engineering the purpose and implementation of the module.

- Micropython source code
- Official documentation, including:
    - .mpy files: link
    - Micropython internals: link
- "Securing a MicroPython System" link
- The collected Raspberry Pi Pico documentation for my test environment link
- Andrew Leech - "Profiling Pathogens with (micro) Python" link
- Kevin McAleer - "Securing Passwords with MicroPython" link
- C. Spindler - "MicroPython used in industrial applications" link
- "MicroPython and the European Space Agency" link

SpeakerBio: Wesley McGrew, Senior Cybersecurity Fellow at MartinFederal

Dr. Wesley McGrew directs research, development, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented on topics of penetration testing and malware analysis at DEF CON and Black Hat USA and taught a self-designed course on reverse engineering to students at Mississippi State University, using real-world, high-profile malware samples. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 14:15-14:59 PDT

Title: RF Attacks on Aviation's Last Line of Defense Against Mid-Air Collisions (TCAS II)
When: Saturday, Aug 10, 14:15 - 14:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Aviation's Traffic Collision Avoidance System (TCAS) II has been touted as a foolproof safety net since its introduction in the 1980s. But what if we told you that this supposedly impenetrable system can be compromised? For years, attacks on TCAS have been mere theoretical exercises, foiled by an (accidental) built in security feature. That is, until now. In this presentation, we'll reveal the first working RF attacks on TCAS II, demonstrating how to hijack collision avoidance displays and create fake Traffic Advisories (TAs) and Resolution Advisories (RAs). We'll walk you through the technical challenges of building the necessary tooling using commercial off-the-shelf hardware.

But that's not all. Our research has also uncovered a second attack capable of remotely disabling an aircraft's TCAS capabilities, rendering it vulnerable to mid-air collisions. The implications are clear: if our findings can be exploited in real-world scenarios, the safety of millions of passengers hangs in the balance. Join us as we lift the lid on this shocking vulnerability and explore the dark side of aviation security.

Speakers: Giacomo Longo,Vincent Lenders

SpeakerBio: Giacomo Longo

Giacomo Longo is a Ph.D. student by day, and a master of mayhem by night. When he's not burrowing through the depths of transportation system security, specifically primary and secondary radar systems, you can find him conjuring chaos as an engineer with a passion for solving what he thinks are the world's most intriguing problems. By harnessing his love for disorder into scientific research, Giacomo is on a mission to uncover the secrets of transportation systems - or at least, that's what he tells his thesis committee. Until the world takes notice, he'll continue to stir up trouble in the name of scientific progress.

SpeakerBio: Vincent Lenders, Cybersecurity Researcher and Head at Cyber-Defence Campus

Vincent Lenders is a cybersecurity researcher from Switzerland where he acts as the Head of the Cyber-Defence Campus. He has a Master and PhD degree from ETH Zurich in electrical engineering. He has over 15 years of practical experience in cybersecurity with a strong focus on the security of wireless networks. He is the co-founder of the OpenSky Network and has published over 150 scientific papers and two books, and presents regularly at cybersecurity conferences including Usenix Secuirty, DEFCON, IEEE S&P, NDSS, ACM CCS.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 10:30-11:25 PDT

Title: RF CTF Kick Off Day 1
When: Friday, Aug 9, 10:30 - 11:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

Presentation to kick off the Radio Frequency Village CTF with helpful tips for new folks.

SpeakerBio: RF Hackers
No BIO available

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 10:30-11:25 PDT

Title: RF CTF Kick Off Day 2
When: Saturday, Aug 10, 10:30 - 11:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:
SpeakerBio: RF Hackers
No BIO available

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 12:30-12:59 PDT

Title: RFID 101
When: Friday, Aug 9, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

You know the sound of *beep... Click* when using a badge to enter a door to a building, but how does this work and how can you hack it? This talk will explain the basics of what's inside the readers and the badges, and how they communicate wirelessly. You will learn about the common tools available (Proxmark, Flipper, Keysy), how to get one and how to use it. We'll talk about techniques to clone badges, and brute force systems to get access you never had in the first place.

Speakers:
Andrew M,Ege Feyzioglu

SpeakerBio:
Andrew M

Andrew M. is a security researcher with a background in the telecommunications industry. His career began at the Blackberry RF test lab, where he honed his expertise in RF testing and wireless protocols. Andrew has continued to expand his skills at a major Satellite Telecom company while moonlighting as a security researcher with an interest in RFID technology and wireless security, consistently expanding his knowledge and skills. He actively contributes to the cybersecurity field through the Physical Security Village educating the public on RFID security best practices and hands-on experimentation, leveraging his extensive experience to drive advancements in wireless security.

SpeakerBio:
Ege Feyzioglu, Physical Security Analyst at GGR Security

Ege is a security researcher specialising in access control systems and electronics. She is currently pursuing a degree in Electrical Engineering and works part-time for GGR Security as a Physical Security Analyst

Return to Index - Add to Google - ics Calendar file

VMV - Friday - 14:30-14:45 PDT

Title: Risk Limiting Audit DEMO by Philip Stark
When: Friday, Aug 9, 14:30 - 14:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

Join the inventor of Risk Limiting Audits for an up close hands on demo of how true Risk Limiting Audits work. Lean the principals and practice of conducting Risk Liming Audits. We will actually be conducting a Risk Limiting Audit during this demo and the audience will participate.

SpeakerBio: Philip Stark

Philip B. Stark is Distinguished Professor of Statistics at the University of California, Berkeley, where he currently focuses on methodology and applications in physical, life, and social sciences. In 2007, he invented risk limiting audits, endorsed by the National Academies of Science, Engineering, and Medicine and the American Statistical Association, among others, and is now required or authorized by law in about 15 states.

Return to Index - Add to Google - ics Calendar file

VMV - Friday - 13:00-13:59 PDT

Title: Risk Limiting Audits From the Source
When: Friday, Aug 9, 13:00 - 13:59 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

Risk Limiting Audits are a powerful statistical technique for determining whether or not election outcomes, determined provisionally by machine counts, are likely to be correct. Join us for an overview of Risk Limiting Audits by the person who invented them. This is an incredible opportunity to understand what a true Risk Limiting Audit is. Many people have misconceptions of what audits and recounts are, and unfortunately do not understand the fundamental basics of what a true audit of an election would look like. Professor Stark will be giving a full overview. Don’t miss out! Following this talk Professor Stark will be giving a Risk Limiting Audit demo in our Voting Machine Lab that we highly recommend you check out!

SpeakerBio: Philip Stark

Philip B. Stark is Distinguished Professor of Statistics at the University of California, Berkeley, where he currently focuses on methodology and applications in physical, life, and social sciences. In 2007, he invented risk limiting audits, endorsed by the National Academies of Science, Engineering, and Medicine and the American Statistical Association, among others, and is now required or authorized by law in about 15 states.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Robo Sumo
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

If you have never participated in a Robo Sumo event before, welcome to the crowd! There are a number of resources online on this topic. We are lucky enough to have Pololu as a local resource. Their office is a short distance from the strip. They have have robots and parts to make robots. They can ship to your hotel if desired. Put something together and bring it down to show off and shove other bots around.

Please follow the "more info" link if you would like to know more.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Robo Sumo
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

If you have never participated in a Robo Sumo event before, welcome to the crowd! There are a number of resources online on this topic. We are lucky enough to have Pololu as a local resource. Their office is a short distance from the strip. They have have robots and parts to make robots. They can ship to your hotel if desired. Put something together and bring it down to show off and shove other bots around.

Please follow the "more info" link if you would like to know more.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Robo Sumo
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-10-01 - Map

Description:

If you have never participated in a Robo Sumo event before, welcome to the crowd! There are a number of resources online on this topic. We are lucky enough to have Pololu as a local resource. Their office is a short distance from the strip. They have have robots and parts to make robots. They can ship to your hotel if desired. Put something together and bring it down to show off and shove other bots around.

Please follow the "more info" link if you would like to know more.

Return to Index - Add to Google - ics Calendar file

PLV - Friday - 12:00-12:45 PDT

Title: Rules All Hackers Must Follow in War
When: Friday, Aug 9, 12:00 - 12:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

As digital technology is changing how militaries conduct war, a trend has emerged in which a growing number of civilians are becoming involved in armed conflicts through digital means. Sitting at some distance from physical hostilities, including outside the countries at war, civilians – including hackers – are conducting a range of cyber operations against their "enemy." One example is the international armed conflict between Russia and Ukraine, where some groups present themselves as a "worldwide IT community" with the mission to, in their words, "help Ukraine win by crippling aggressor economies, blocking vital financial, infrastructural and government services, and tiring major taxpayers." Others have reportedly "called for and carried out disruptive – albeit temporary – attacks on hospital websites in both Ukraine and allied countries," among many other operations. In this session, the International Committee of the Red Cross will highlight that there are legal limits in warfare, and will set out several international humanitarian law (IHL)-based rules that all hackers who carry out operations in the context of an armed conflict must comply with. The session will also discuss why it is a State's responsibility to restrain hackers engaging in those conflicts.

SpeakerBio: Dr. Kosuke Onishi, Legal Advisor at International Committee of the Red Cross

Dr. Kosuke Onishi is a legal adviser for the International Committee of the Red Cross (ICRC) at the Permanent Observer Mission to the United Nations in New York. Prior to this, he was a legal adviser for the ICRC Regional Delegation in Washington D.C. Dr. Onishi has also taught international law at Osaka University and Aichi Prefectural University as an adjunct lecturer. He holds a B.A. in law from Doshisha University, an M.A. in global politics and law from Doshisha and Sheffield Universities (dual degree), an LL.M. in public international law from Leiden University, and an LL.D. from Doshisha University.

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 13:10-13:50 PDT

Title: Runtime Reachability: Prioritizing Vulnerabilities with eBPF & Continuous Profiling
When: Saturday, Aug 10, 13:10 - 13:50 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

As security engineers, managing risk means making informed decisions about which vulnerabilities to address first. We are often too time constrained, and the signal-to-noise ratio of current SAST/SCA tooling is too low.

This talk introduces "Runtime Reachability," a novel approach that leverages Continuous Profiling via eBPF to quantify how often a vulnerable method/codepath is called, in actual production usage. By understanding the runtime behavior of applications, security teams can effectively filter out low-likelihood vulnerabilities, prioritize fixes more effectively, reduce toil & the overall risk to their organization.

SpeakerBio: Sam "Frenchie" Stewart

Frenchie is the founder & CEO of Ensignia Security. Previously: InfraSec @ Brex/Cruise/Culture Amp. He has previously presented on cloud, cluster, container & CI/CD security (anything starting with a C, really) at BSidesSF/Melbourne/Canberra, ProjectDiscovery's Hardly Strictly Security and Kiwicon conferences, amongst others. Frenchie is far too biased to answer this question, and instead chooses to break the 4th wall.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 11:00-11:50 PDT

Title: RustOps
When: Saturday, Aug 10, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Join me for a hands-on workshop delving into the fundamentals of the Rust programming language and its application in malware development. Designed for both curious beginners and seasoned developers, this session will cover the basics of Rust while also exploring the unique features that make Rust a powerful tool for crafting malware. Through guided exercises and real-world examples, participants will gain practical insights into how Rust can be leveraged to develop sophisticated, stealthy, and malicious software.

SpeakerBio: Jose Plascencia
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:00-12:59 PDT

Title: Safe Hacking
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Hack a (not-so) smart safe and win prizes from TCM Security! Attendees will be guided through a hands-on lab that demonstrates common tools and techniques to unpack and analyze firmware, hunt for files of interest, and reverse engineer binaries and libraries. In addition, you will learn how to trace functionality in IoT devices to their underlying binaries and libraries and further reverse engineer these to hunt for common vulnerabilities. By using these techniques, you will be able to find the vulnerable section of code in the smart safe and craft an exploit that will allow you to access the safe and win the loot inside.

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-17:59 PDT

Title: Safe Hacking
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Hack a (not-so) smart safe and win prizes from TCM Security! Attendees will be guided through a hands-on lab that demonstrates common tools and techniques to unpack and analyze firmware, hunt for files of interest, and reverse engineer binaries and libraries. In addition, you will learn how to trace functionality in IoT devices to their underlying binaries and libraries and further reverse engineer these to hunt for common vulnerabilities. By using these techniques, you will be able to find the vulnerable section of code in the smart safe and craft an exploit that will allow you to access the safe and win the loot inside.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 10:00-17:59 PDT

Title: Safe Hacking
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Hack a (not-so) smart safe and win prizes from TCM Security! Attendees will be guided through a hands-on lab that demonstrates common tools and techniques to unpack and analyze firmware, hunt for files of interest, and reverse engineer binaries and libraries. In addition, you will learn how to trace functionality in IoT devices to their underlying binaries and libraries and further reverse engineer these to hunt for common vulnerabilities. By using these techniques, you will be able to find the vulnerable section of code in the smart safe and craft an exploit that will allow you to access the safe and win the loot inside.

Return to Index - Add to Google - ics Calendar file

LPV - Friday - 12:00-12:59 PDT

Title: Safecracking for Everyone
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Learn the inner workings and vulnerabilities of mechanical combination safe locks! Safe manipulation is an underrated aspect of locksport and this talk will guide you through the ins and outs of how to do it.

SpeakerBio: Jared Dygert

Jared is a long time lock sport enthusiast and an instructor at a locksmithing school on safe manipulation and lockpicking. He has been opening locks and breaking security for roughly 15 years. His other hobbies include rock climbing and 3D printing.

Return to Index - Add to Google - ics Calendar file

LPV - Friday - 13:00-15:59 PDT

Title: Safecracking Practical Demonstration
When: Friday, Aug 9, 13:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03-A - Map

Description:

Join us at the lock pick village tables after Jared's talk on safe manipulation for some hands on practice!

SpeakerBio: Jared Dygert

Jared is a long time lock sport enthusiast and an instructor at a locksmithing school on safe manipulation and lockpicking. He has been opening locks and breaking security for roughly 15 years. His other hobbies include rock climbing and 3D printing.

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 10:00-10:30 PDT

Title: SBOMs the Hard Way: Hacking Bob the Minion
When: Saturday, Aug 10, 10:00 - 10:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

This presentation delves into the intricate process of generating a Software Bill of Materials (SBOM) for the Bob the Minions WiFi router by Davolink—a device whose firmware isn't publicly available. Traditional SBOM creation methods rely on readily accessible firmware, but Davolink's restricted release policies necessitated an unconventional approach. This talk covers the step-by-step journey of hardware disassembly, firmware extraction via SPI flash and JTAG/SWD interfaces, and the tools and techniques employed. Finally, we'll demonstrate how the recovered firmware is used to generate a comprehensive SBOM, highlighting any security vulnerabilities discovered and reported to the vendor. This session aims to provide attendees with practical insights into overcoming SBOM generation challenges in the IoT domain through hands-on hardware hacking, and leveraging the firmware and SBOMs for vulnerability discovery, as well as security improvement.

SpeakerBio: Larry Pesce, Co-Founder and Co-Host at "Paul's Security Weekly" podcast

A self-professed, lifelong "tinkerer and explorer," Larry always wanted to know how things work. "I found myself getting to engage in deep dives of technology from an early age: My dad built the family television from a kit, and I helped. It caught fire. Twice. I helped fix it both times." The help and advice received from the infosec community throughout his career inspired him to share what he had learned to help others secure their networks and improve their craft. Part of that ongoing sharing has been as the co-founder and co-host of the international award winning Paul's Security Weekly podcast for more than 17 years. Larry has spent the last 15 years as a penetration tester, spending lots of time focused on Healthcare, ICS/OT, Wireless, and IoT/IIoT/Embedded Devices, but now focuses his efforts on securing the software supply chain at Finite State.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 14:00-15:45 PDT

Title: SCAGoat - Exploiting Damn Vulnerable SCA Application
When: Friday, Aug 9, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W305 - Map

Description:

SCAGoat is a deliberately insecure web application designed for learning and testing Software Composition Analysis (SCA) tools. It offers a hands-on environment to explore vulnerabilities in Node.js and Java Springboot applications, including actively exploitable CVEs like CVE-2023-42282 and CVE-2021-44228 (log4j). This application can be utilized to evaluate various SCA and container security tools, assessing their capability to identify vulnerable packages and code reachability. As part of our independent research, the README includes reports from SCA tools like semgrep, snyk, and endor labs. Future research plans include incorporating compromised or malicious packages to test SCA tool detection and exploring supply chain attack scenarios.

Speakers: Hare Krishna Rai,Prashant Venkatesh

SpeakerBio: Hare Krishna Rai, Product Security Engineer

As a Product Security Engineer, Hare Krishna Rai's passion for cybersecurity drives him to excel in various areas. He specializes in conducting penetration testing, actively participates in security Capture The Flag (CTF) competitions, and performs code reviews to ensure secure code development. His expertise extends to leveraging Static Application Security Testing (SAST) techniques in languages like Java, Python, JavaScript, JSP, among others.

SpeakerBio: Prashant Venkatesh, Manager, Product Security

Prashant Venkatesh is an information security expert with over 20 years of experience. He presently works as Manager, Product Security at an ecommerce company. Prashant is an enthusiastic participant in the field who consistently coordinates, reviews papers, and presents his work at numerous InfoSec conferences, including Blackhat Nullcon and c0c0n. He is also active through the OWASP Bay Area chapter Leadership and is co-founder of the annual Seasides Conference in India.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 13:15-13:45 PDT

Title: SDLC Nightmares - Defeating Secure Code Review GPT Hallucinations
When: Friday, Aug 9, 13:15 - 13:45 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

In this talk, we will discuss the strengths and limitations of LLMs for code analysis tasks like code search and code clone detection. We will show when the LLMs make mistakes and what kinds of mistakes they make. For example, we observe that the performance of popular LLMs heavily relies on the well-defined variable and function names, therefore, they will make mistakes when some misleading variable name is given. Anyone interested in exploring the intersection of AI and code security analysis can attend this talk.

Speakers:
Wang Zhilong,Xinzhi Luo

SpeakerBio: Wang Zhilong

Now security engineer in industry.

Ph.D. degree obtained from Penn State University in 2023.

Master degree obtained from Nanjing University in 2019.

SpeakerBio: Xinzhi Luo

Xinzhi (April) Luo is a Carnegie Mellon University graduate with over three years of experience in information security. She combines technical expertise with a passion for sci-fi, often writing original stories. She is dedicated to innovative cybersecurity solutions.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 16:00-16:45 PDT

Title: Secrets and Shadows: Leveraging Big Data for Vulnerability Discovery at Scale
When: Saturday, Aug 10, 16:00 - 16:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

When we consider the conventional approaches to vulnerability discovery, be it in software or websites, we tend to confine ourselves to a specific target or platform. In the case of software, we might reverse engineer an application's attack surfaces for untrusted input, aiming to trigger edge cases. For websites, we might enumerate a domain for related assets and seek out unpatched, less defended, or occasionally abandoned resources.

This presentation explores the untapped potential of scaling security research by leveraging unconventional data sources. We'll walk through design flaws that enable two examples: forgotten cloud assets and leaked secrets. Instead of starting with a target and finding vulnerabilities, we'll find vulnerabilities and relate them to our targets. We won't just stop at discovery. We'll also discuss the incentives that create them and how to solve the ecosystem issues as an industry.

While you can't easily scale every issue, this project has led to tens of thousands of highly significant yet seemingly trivial weaknesses in some of the world's largest organizations. Prepare to shift your perspective on vulnerability discovery, learn scalable approaches to address commonly overlooked bugs, and understand how even the simplest misconfiguration can have a devastating impact.

- Toomey, Patrick. “Behind the Scenes of Github Token Scanning.” The GitHub Blog, 17 Oct. 2018, link.
- Meli, Michael, et al. “How Bad Can It Git? Characterizing Secret Leakage in Public Github Repositories.” Proceedings 2019 Network and Distributed System Security Symposium, 19 Feb. 2019, link.
- Awslabs. “Awslabs/Git-Secrets: Prevents You from Committing Secrets and Credentials into Git Repositories.” GitHub, 2015, link.
- Rice, Zachary. “Zricethezav/Gitleaks: Scan Git Repos (or Files) for Secrets Using Regex and Entropy.” GitHub, 2018, link.
- Ballenthin, Willi, and Moritz Raabe. “Mandiant/Flare-Floss: Flare Obfuscated String Solver - Automatically Extract Obfuscated Strings from Malware.” GitHub, 2016, link.
- Squarcina, Marco, et al. “Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web.” USENIX Security Symposium, vol. 30, Aug. 2021, pp. 2917–2934.
- MDN contributors. “Subdomain Takeovers - Web Security | MDN.” Developer.mozilla.org, 14 Oct. 2021, link.
- “Prevent Subdomain Takeovers with Azure DNS Alias Records and Azure App Service’s Custom Domain Verification.” Learn.microsoft.com, Microsoft, 16 June 2020, link.
- Shah, Shubham. “Eliminating Dangling Elastic IP Takeovers with Ghostbuster.” Assetnote, 13 Feb. 2022, link.
- Claudius, Jonathan. “‘Deep Thoughts’ on Subdomain Takeover Vulnerabilities.” Claudijd.github.io, 3 Feb. 2017, link.
- Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019). link
- Hallam-Baker, Phillip, et al. “RFC 8659 - DNS Certification Authority Authorization (CAA) Resource Record.” Datatracker.ietf.org, IETF, Nov. 2019, link.

SpeakerBio: Bill Demirkapi, Independent Security Researcher

Bill is an independent security researcher with a passion for finding bugs at scale. His interests include reverse engineering and vulnerability research, ranging from low-level memory corruption to systemic flaws with catastrophic consequences. He started his journey in high school and has since published his work at internationally-recognized conferences like DEF CON and Black Hat USA. In his pursuit to make the world a better place, Bill constantly looks for the next significant vulnerability, following the motto "break anything and everything".

MISC - Sunday - 10:00-10:59 PDT

Title: Secure From Scatch
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Want to learn how to stop hackers in their tracks? Come to the Secure From Scratch coding workshop. Learn what you need to know to write secure code from the very first line of code. It's surprisingly easy! Plus, you'll get to try your hand at hacking, discovering how attackers think so you can build defences against them. (Some coding knowledge in Python is recommended. You should know loops, if statements, arrays, and functions.)

Return to Index - Add to Google - ics Calendar file

ESV - Friday - 10:00-17:59 PDT

Title: Secure Microcontroller Workshop
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Come try a hands-on workshop on embedded computing using the new RP2350 processor from Raspberry Pi. Lean about the security architecture in modern embedded microprocessors and tinker with it in person! Think you have what it takes to break our stuff? Come learn, say hi and give it a try!

Return to Index - Add to Google - ics Calendar file

ESV - Saturday - 10:00-17:59 PDT

Title: Secure Microcontroller Workshop
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Come try a hands-on workshop on embedded computing using the new RP2350 processor from Raspberry Pi. Lean about the security architecture in modern embedded microprocessors and tinker with it in person! Think you have what it takes to break our stuff? Come learn, say hi and give it a try!

Return to Index - Add to Google - ics Calendar file

ESV - Sunday - 10:00-12:59 PDT

Title: Secure Microcontroller Workshop
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Come try a hands-on workshop on embedded computing using the new RP2350 processor from Raspberry Pi. Lean about the security architecture in modern embedded microprocessors and tinker with it in person! Think you have what it takes to break our stuff? Come learn, say hi and give it a try!

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 12:00-12:59 PDT

Title: Secure the Skies: A Modern Android Security Research Framework for Drone Ground Control Stations and Applications

When: Saturday, Aug 10, 12:00 - 12:59 PDT

Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

Drones, also known as unmanned aerial vehicles (UAVs), are becoming increasingly popular for various applications, from delivery and surveillance to emergency response and military support. While traditionally controlled by dedicated remote controllers (ground control stations), Android is emerging as a powerful platform for drone development and operation. For example, some drone manufacturers, like DJI, have developed their own custom Android-based operating systems (OS) for their drones. Open-source Android-based flight control software like QGroundControl and Mission Planner are also available, allowing developers to build custom drone control applications. With the growing reliance on Android within the drone market, the necessity to understand the landscape of Android-based vulnerabilities and exposure has become more important than ever before, especially to ensure secure, safe, and reliable drone operations.

SpeakerBio: Jonathan Waterman

Jonathan Waterman has spent the last 15 years focused on cyber security, spanning both defensive and offensive security. His career started as an ISSM verifying network policies and secure procedures. After obtaining his B.S. in Computer Science from Clarkson University in 2012, his focus became the integrity of applications and sanitization of data. He went from testing and finding ways to bypass secure systems, to writing and enhancing network monitoring systems. Over the course of his career, he worked with the Department of Defense and other defense contracting companies enhancing security postures. For the last 2 years, he has focused specifically on IoT and Android based devices. Many of the programs he worked on were a combination of black and white box testing, requiring expertise in reverse engineering, vulnerability research, binary exploitation, and penetration testing. Currently he serves as a principal security research engineer at Dark Wolf Solutions, leading the Android vulnerability research team.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 10:00-10:20 PDT

Title: Securing CCTV Cameras Against Blind Spots
When: Friday, Aug 9, 10:00 - 10:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

In recent years, CCTV footage has been integrated in systems to observe areas and detect traversing malicious actors (e.g., criminals, terrorists). However, this footage has "blind spots", areas where objects are detected with lower confidence due to their angle/distance from the camera.

In this talk, we investigate a novel side effect of object detection in CCTV footage; location-based confidence weakness.

We demonstrate that a pedestrian's position (distance, angle, height) in footage impacts an object detector's confidence.

We analyze this phenomenon in four lighting conditions (lab, morning, afternoon, night) using five object detectors (YOLOv3, Faster R-CNN, SSD, DiffusionDet, RTMDet).

We then demonstrate this in footage of pedestrian traffic from three locations (Broadway, Shibuya Crossing, Castro Street), showing they contain "blind spots" where pedestrians are detected with low confidence. This persists across various locations, object detectors, and times of day. A malicious actor could take advantage of this to avoid detection.

We propose TipToe, a novel evasion attack leveraging "blind spots" to construct a minimum confidence path between two points in a CCTV-recorded area. We demonstrate its performance on footage of Broadway, Shibuya Crossing, and Castro Street, observed by YOLOv3, Faster R-CNN, SSD, DiffusionDet, and RTMDet.

TipToe reduces max/average confidence by 0.10 and 0.16, respectively, on paths in Shibuya Crossing observed by YOLOv3, with similar performance for other locations and object detectors.

1. Artificial intelligence in medicine: A comprehensive survey of medical doctor’s perspectives in Portugal link, (Accessed 09-10-2023).
2. The impact of artificial intelligence along the insurance value chain and on the insurability of risks - The Geneva Papers on Risk and Insurance - Issues and Practice link, (Accessed 09-10-2023).
3. R. Chopra and G. D. Sharma, “Application of artificial intelligence in stock market forecasting: A critique, review, and research agenda,” Journal of Risk and Financial Management, vol. 14, no. 11, 2021.link
4. [B. B. Elallid, N. Benamar, A. S. Hafid, T. Rachidi, and N. Mrani, “A comprehensive survey on the application of deep and reinforcement learning approaches in autonomous driving,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 9, pp. 7366–7390, 2022. (Online). Available: link
5. I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial networks,” 2014.
6. I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” 2015.
7. A. Kurakin, I. Goodfellow, and S. Bengio, “Adversarial examples in the physical world,” 2017.
8. A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, “Adversarial attacks and defences: A survey,” 2018.
9. A. Athalye, L. Engstrom, A. Ilyas, and K. Kwok, “Synthesizing robust adversarial examples,” 2018.
10. M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, “Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’16. New York, NY, USA: Association for Computing Machinery, 2016, p. 1528–1540. (Online). Available: link
11. Z. Zhou, D. Tang, X. Wang, W. Han, X. Liu, and K. Zhang, “Invisible mask: Practical attacks on face recognition with infrared,” 2018.
12. S. Komkov and A. Petiushko, “AdvHat: Real-world adversarial attack on ArcFace face ID system,” in 2020 25th International Conference on Pattern Recognition (ICPR). IEEE, jan 2021. (Online). Available: link

13. B. Yin, W. Wang, T. Yao, J. Guo, Z. Kong, S. Ding, J. Li, and C. Liu, “Adv-makeup: A new imperceptible and transferable attack on face recognition,” in Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, IJCAI-21, Z.- H. Zhou, Ed. International Joint Conferences on Artificial Intelligence Organization, 8 2021, pp. 1252–1258, main Track. (Online). Available: link
14. A. Zolfi, S. Avidan, Y. Elovici, and A. Shabtai, “Adversarial mask: Real-world universal adversarial attack on face recognition model,” 2022.
15. C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, “Darts: Deceiving autonomous cars with toxic signs,” 2018.
16. Y. Zhao, H. Zhu, R. Liang, Q. Shen, S. Zhang, and K. Chen, “Seeing isn’t believing: Towards more robust adversarial attack against real world object detectors,”Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019. (Online). Available: link
17. G. Lovisotto, H. Turner, I. Sluganovic, M. Strohmeier, and I. Martinovic, “SLAP: Improving physical adversarial examples with Short-Lived adversarial perturbations,” in 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, Aug. 2021, pp. 1865–1882. (Online). Available: link
18. T. Sato, J. Shen, N. Wang, Y. Jia, X. Lin, and Q. A. Chen, “Dirty road can attack: Security of deep learning based automated lane centering under Physical-World attack,” in 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, Aug. 2021, pp. 3309–3326. (Online). Available: link
19. W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, “I can see the light: Attacks on autonomous vehicles using invisible lights,” in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’21. New York, NY, USA: Association for Computing Machinery, 2021, p. 1930–1944. (Online). Available: link
20. S.-T. Chen, C. Cornelius, J. Martin, and D. H. Chau, “ShapeShifter: Robust physical adversarial attack on faster r-CNN object detector,” in Machine Learning and Knowledge Discovery in Databases. Springer International Publishing, 2019, pp. 52–68. (Online). Available: link
21. K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, “Robust physical-world attacks on deep learning models,” 2018.
22. S. Thys, W. V. Ranst, and T. Goedemé, “Fooling automated surveillance cameras: adversarial patches to attack person detection,” 2019.
23. Z. Wu, S.-N. Lim, L. Davis, and T. Goldstein, “Making an invisibility cloak: Real world adversarial attacks on object detectors,” 2020.
24. R. M. Oza, A. Geisen, and T. Wang, “Traffic sign detection and recognition using deep learning,” in 2021 4th International Conference on Artificial Intelligence for Industries (AI4I), 2021, pp. 16–20.

SpeakerBio: Jacob Shams, Ph.D. Researcher at Cyber@Ben-Gurion University

Jacob Shams is a Ph.D. student at Ben-Gurion University of the Negev (BGU). His work addresses the security of AI models and systems, model extraction attacks, deep neural network (DNN) watermarking, and robustness of computer vision (CV) models.

Jacob is a Ph.D. researcher at Cyber@Ben-Gurion University (CBG) and is working on multiple research projects in the area of AI security. Jacob holds a B.Sc. in Software Engineering from BGU and an M.Sc. in Software and Information Systems Engineering from BGU.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 11:00-11:30 PDT

Title: Securing Frontends at Scale: Paving our Way to the Post-XSS World
When: Friday, Aug 9, 11:00 - 11:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Cross-site scripting (XSS) remains a top web vulnerability. Google has invested heavily in defenses, and in this talk, we'll share our blueprint for protecting your code. We'll discuss how we implemented runtime and compile-time protections across hundreds of products used by billions, highlighting technical lessons and best practices. We'll also glimpse into the future of anti-XSS defenses and explore how we can make the web safer for everyone.

Speakers:Aaron Shim,jen-ozmen

SpeakerBio: Aaron Shim

Aaron is a Senior Software Engineer at Google working on product security across all of Google's user facing webapps. Bridging the gap between security and development work, he has worked on product teams at both Google and Microsoft in the past, including Docs, GCP, and Visual Studio. He is extremely passionate about the developer experience and committed to empowering every dev to build the most secure and delightful products.

SpeakerBio: jen-ozmen

Jen Ozmen is a Software Engineer at Google, where she works on the Information Security Engineering team, focusing on defense-in-depth mechanisms against common web vulnerabilities. She is passionate about building secure and reliable software, and she is always looking for new ways to improve the security of Google's web ecosystem. She is an active member of the tech community and enjoys sharing her knowledge through presentations at conferences like LibertyJS and Frontrunners DC.

Return to Index - Add to Google - ics Calendar file

AIxCC - Saturday - 10:00-10:45 PDT

Title: Securing Health Care: AIxCC, DIGIHEALS, and UPGRADE
When: Saturday, Aug 10, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

ARPA-H accelerates better health outcomes for everyone by supporting the development of high-impact solutions to society's most challenging health problems. Join us in discussing why strong cybersecurity security is a critical piece of healthcare innovation and how ARPA-H is enabling this through the AIxCC, DIGIHEALS, and UPGRADE programs.

Speakers: Dr. Jennifer Roberts,Dr. Susan Coller Monarez,Andrew Carney

SpeakerBio: Dr. Jennifer Roberts, Office Director of Resilient Systems at ARPA-HPhD

Dr. Jennifer Roberts joined ARPA-H in February 2023 from the White House Office of Science and Technology Policy, where she was the assistant director of Health Technologies. She has a broad background in both engineering and computer science and has overseen research programs and strategy development on topics such as cyber security, healthcare data interoperability, artificial intelligence for synthetic biology, and information integrity.

Before joining the White House, Roberts worked for the Defense Advanced Research Projects Agency as deputy director of the Information Innovation Office. During this time, she received the prestigious Superior Public Service Medal for her contributions to the fields of artificial intelligence and cyber security. Roberts has a Ph.D. in computer science from MIT, which she attended as both a National Science Foundation and Hertz Foundation Fellow.

SpeakerBio: Dr. Susan Coller Monarez, Deputy Director at ARPA-HPhD

Dr. Susan Coller Monarez is a globally recognized leader with more than 20 years of experience in health innovation. Throughout her career, Monarez has focused on understanding the critical challenges within the health ecosystem and the greatest opportunities for innovation to meet these challenges. Prior to serving as ARPA-H deputy director, Monarez led innovation at the Health Resources and Services Administration, focused on ethical use of AI/ML to support improved health outcomes, novel approaches to addressing social determinants of health, expanding access to behavioral health, ending the opioid epidemic, addressing health equity gaps in maternal and infant mortality, and improving the country’s organ donation and transplantation programs.

Monarez has also served at the White House as the assistant director for National Health Security and International Affairs in the Office of Science and Technology Policy and as the director of Medical Preparedness Policy on the National Security Council. In both White House roles, she led efforts to enhance the nation’s biomedical innovation capabilities including combating antibiotic resistant bacteria and MDR/XDR TB, expanding telehealth and remote patient monitoring, establishing safeguards to ensure personal health data privacy, and improving pandemic preparedness. Monarez led the development of several Presidential-level national strategies, action plans, and policy directives related to domestic and global health.

Monarez also served in leadership positions at the Homeland Security Advanced Research Projects Agency within the Department of Homeland Security and the Biomedical Advanced Research Projects Agency within HHS. In addition to leadership roles within the federal government, Monarez has served on numerous advisory panels, including for the National Academies of Science, the National Science Advisory Board for Biosecurity, and the Organization for Economic Cooperation and Development. Monarez has also served as the U.S. representative on several international cooperative initiatives including with the European Union, Canada, France, the Netherlands, and the United Kingdom in bilateral and multilateral engagements.

Monarez was a Science and Technology Policy fellow with the American Association for the Advancement of Science. Prior to government service, Monarez was a postdoctoral fellow and graduate student, respectively, at Stanford University and the

University of Wisconsin, where she focused on technology development to prevent, diagnose, and treat infectious diseases with a focus on people living in low- and middle-income countries.

SpeakerBio: Andrew Carney, Program Manager at Advanced Research Projects Agency for Health (ARPA-H)

Andrew Carney joined ARPA-H in July 2023 from HSBC's Cybersecurity Science and Analytics group, where he worked as a principal researcher. He has over 15 years of experience in software and hardware vulnerability research, technical education and training, and management of research and development teams.

In addition to his role as program manager with ARPA-H, Carney holds a joint program manager appointment with the Defense Advanced Research Projects Agency (DARPA) for the AI Cyber Challenge (AIxCC), a competition focused on securing software in critical infrastructure. Before HSBC, Carney was a technical advisor and contractor for the Defense Advanced Research Projects Agency (DARPA). At DARPA, he supported research efforts focused on reverse engineering, program analysis, human-machine teaming, and automated program repair. Throughout his career, Carney has been involved in competitive hacking (called Capture the Flag, or CTF) as both a player and a competition organizer. He holds a master's degree in computer science from The Johns Hopkins University.

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 10:00-11:59 PDT

Title: Securing the Cloud with Cloud Threat Intelligence and Open Source Security
When: Saturday, Aug 10, 10:00 - 11:59 PDT
Where: LVCC West/Floor 3/W309 - Map

Description:

-Introductions [5 minutes] -Cloud Threat Intelligence [5 minutes] -Threat Brief on Cloud Focused Adversaries: SCATTERED SPIDER -Cloud Security Assessments [5 minutes] -Introduction to Prowler -SadCloud Introduction [5 minutes] -Demo of Running Sadcloud [5 minutes] -Hands-On Exercise [40 minutes] -Participants given the option: -Create AWS Account -Use Access Keys
-Participants setup AWS CLI -Participants run Sadcloud -Demo of Running Prowler [10 minutes] -Hands-On Exercise [30 minutes] -Participants run Prowler -Summary Review of Prowler output [10 minutes]
-Debrief/Q&A [5 minutes]

Please download and install terraform and python requirements noted below for this training: Sadcloud Requirements: Terraform version 0.12 or greater Terraform download: https://developer.hashicorp.com/terraform/install

Prowler Requirements: Python version 3.9, 3.10, or 3.11 Python download: https://www.python.org/downloads/

Attend this talk to get hands-on experience setting up an AWS environment, running cloud security tools to analyze its security, and mapping its security configuration against TTPs of a cloud conscious adversary. Cloud cyberattacks targeting enterprise environments have nearly tripled this past year, and cloud misconfigurations have become an open door to threat actors. Understanding cloud threat actors and how they are breaching cloud environments will help security professionals defend organizations with a cloud footprint. This workshop will showcase how to defend against the top cloud conscious adversaries and the most popular cyber attacks. During the workshop, participants will set up a demo AWS environment, identify security misconfigurations using Prowler, and map those findings to TTPs of a cloud conscious threat actor, SCATTERED SPIDER. Come to this workshop to gain practical skills that empower you to better secure your organization's cloud environment against the modern adversary.

Speakers: Natalie Simpson,Nivedita (Nivu) Jejurikar

SpeakerBio: Natalie Simpson
No BIO available
SpeakerBio: Nivedita (Nivu) Jejurikar, Senior Consultant at Mandiant

Nivu Jejurikar is a Senior Consultant at Mandiant, part of Google Cloud. In her role, Nivu advises organizations of various sizes and industry verticals on cybersecurity topics, including cloud security. Nivu has previously worked at CrowdStrike and Deloitte Cyber. She holds the Security+, CEH, and AWS Cloud Practitioner certifications. In her spare time, she enjoys reading fiction books and spending time outdoors.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 11:00-11:50 PDT

Title: Securing the Future with CoSAI: Identified Technical Workstreams and Call for Contributions
When: Saturday, Aug 10, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

Join members of the newly launched OASIS Coalition for Secure AI (CoSAI) Open Project (https://www.coalitionforsecureai.org). This is an engaging forum hosted by the Red Team Village in collaboration with the AI Village.

CoSAI's members include Amazon, Anthropic, Chainguard, Cisco, Cohere, GenLab, Google, IBM, Intel, Microsoft, NVIDIA, OpenAI, PayPal, and Wiz.

Panelists will discuss the first three technical workstreams that the group has identified:

- Software Supply Chain Security for AI Systems: Enhancing composition and provenance tracking to secure AI applications.
- Preparing Defenders for a Changing Cybersecurity Landscape: Addressing investments and integration challenges in AI and classical systems.
- AI Security Governance: Developing best practices and risk assessment frameworks for AI security.

Also, learn how the CoSAI goals differ from other AI efforts and plans for collaboration. The panelists will emphasize the importance of diverse community input and will host an interactive segment on how you can contribute. Whether you are red-teaming an AI model or implementing AI-powered tools, don't miss this opportunity to gain insights into this open project and learn how you can contribute to shaping a secure AI future

Speakers: Omar Santos,Dan McInerney,Daniel Rohrer,Jay White,Paul Vixie,Sarah Novotny

SpeakerBio: Omar Santos
No BIO available
SpeakerBio: Dan McInerney
No BIO available
SpeakerBio: Daniel Rohrer
No BIO available
SpeakerBio: Jay White
No BIO available
SpeakerBio: Paul Vixie
No BIO available
SpeakerBio: Sarah Novotny
No BIO available

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 10:00-10:55 PDT

Title: Securing the Harvest: Cyber Defense for Agricultural Control Systems
When: Saturday, Aug 10, 10:00 - 10:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

In the digital age, the agriculture industry has embraced advanced technologies to enhance productivity and efficiency. Central to this transformation are Industrial Control Systems (ICS), which manage everything from irrigation and fertilization to harvesting and storage. However, the integration of ICS in agriculture has also introduced a new vector of vulnerabilities and cyber threats.

This presentation will delve into the critical need to secure ICS in the agriculture sector against an ever-growing array of cyber threats. We will explore the unique challenges that agriculture faces, including the dispersed nature of operations, the integration of legacy systems with modern technologies, and the reliance on remote access and IoT devices.

SpeakerBio: Ray Baeza, Founder at Agriculture Defense Group

Ray Baeza is the founder of Agriculture Defense Group, specializing in cybersecurity services for the agriculture industry. Hailing from Davis, CA, Ray grew up immersed in agriculture. With over 6 years of experience as an ICS cybersecurity engineer, Ray has honed expertise in ICS detection engineering and incident response. Driven by a passion for ICS technologies and the agriculture industry, he is dedicated to safeguarding agricultural systems from cyber threats.

Return to Index - Add to Google - ics Calendar file

SEV - Saturday - 12:30-12:59 PDT

Title: SECV - Break / Networking
When: Saturday, Aug 10, 12:30 - 12:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Time to mingle! Discover who can tell the best dad jokes. We're taking a quick break - be back soon!

Return to Index - Add to Google - ics Calendar file

SEV - Saturday - 15:00-15:30 PDT

Title: SECV - Break / Networking
When: Saturday, Aug 10, 15:00 - 15:30 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Time to mingle! Discover who can tell the best dad jokes. We're taking a quick break - be back soon!

Return to Index - Add to Google - ics Calendar file

SEV - Sunday - 10:00-11:30 PDT

Title: SECVC Awards & Competitor Panel + Youth Challenge Awards
When: Sunday, Aug 11, 10:00 - 11:30 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

See who won in our village! During this time we'll present the Youth Challenge winner, the #SECVC 1st and 2nd place winners, as well as the much-coveted Dundies! Then stick around as we have a panel interview with the winners to hear their story about their path to victory!

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 14:00-14:50 PDT

Title: Seeing the Unseen: An Evaluation of Active Scanning in ICS Environments
When: Saturday, Aug 10, 14:00 - 14:50 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The National Renewable Energy Laboratory's Clean Energy Cybersecurity Accelerator (CECA) program focuses on accelerating the deployment of innovative OT security solutions in the electric grid. Sponsored by the Department of Energy and utility partners, CECA collaborates with utility sponsors to prioritize cybersecurity gaps and evaluate emerging solutions focused on those gaps. The second cohort of CECA addressed the challenge of OT asset management, particularly incomplete system visibility in Industrial Control Systems (ICS). This presentation covers CECA's evaluation of runZero, a product that enhances asset visibility through active scanning. The evaluation process involved rigorous, repeatable testing in a controlled environment to assess the product's ability to accurately identify devices and its impact on device operation. We will discuss the results of this testing, demonstrating how active scanning can be safe and effective for improving asset visibility. Additionally, we will delve into CECA's testing philosophy and approach, providing insights into our evaluation process and how it ensures the reliability and efficacy of new cybersecurity solutions.

SpeakerBio: Jennifer Guerra, Cybersecurity Researcher at National Renewable Energy Laboratory (NREL)

Jennifer Guerra is a cybersecurity researcher at the National Renewable Energy Laboratory (NREL), where she focuses on building representative architectures and designing scientific evaluations for novel OT solutions. She currently serves as a technical lead for the Clean Energy Cybersecurity Accelerator (CECA), which advances cyber innovation to defend modern, renewable energy technologies against high-priority cybersecurity risks to the energy sector.

Prior to joining NREL, she served as a cyber-physical systems security researcher at the Oak Ridge National Laboratory (ORNL) coordinating cyber actions and emanation detection on an energized electric power system. She holds an M.S. in Computer Science and B.S. in Criminal Justice and Psychology which have influenced the unique perspective she brings to persistent and emerging ICS security challenges.

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Selfie with a CubeSat
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Come take a picture with a CubeSat. And while you're there, learn a few things about it.

SpeakerBio: CalPoly
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Selfie with a CubeSat
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Come take a picture with a CubeSat. And while you're there, learn a few things about it.

SpeakerBio: CalPoly
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Selfie with a CubeSat
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Come take a picture with a CubeSat. And while you're there, learn a few things about it.

SpeakerBio: CalPoly
No BIO available

Return to Index - Add to Google - ics Calendar file

DL - Friday - 12:00-13:45 PDT

Title: Serberus
When: Friday, Aug 9, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W308 - Map

Description:

The Serberus is a serial Man-in-the-Middle hardware hacking tool designed to connect to embedded devices . It has 4 channels and has headers to interface with up to 3 UARTs simultaneously and also has the ability to connect to JTAG, SPI, I2C and SWD interfaces. During this talk I will introduce the Serberus and what makes it different than other, similar tools. It has a level shifter and switch to allow you to connect to logic voltages of 1.8, 2.5 and 3.3v or any arbitrary voltage between 1.65v and 5.5v, matching that of your target. The Serberus is unique in that it was designed to use open source tools like the Akheron proxy in order to MitM serial communications. I will demonstrate the Serberus connecting to a wifi router, to a JTAG, I2C or SPI target and I will also show the MitM capabilities on the serial connection between an aircraft transponder and its avionics system. The Serberus project is free and open source with all board layouts, gerbers and schematics published.

SpeakerBio: Patrick Kiley, Principal Consultant at Mandiant

Principal Consultant at Mandiant (a division of Google Cloud) has over 20 years of information security experience working with both private sector employers and the Department of Energy/National Nuclear Security Administration (NNSA). Patrick has spoken at DEF CON, BlackHat, Bsides and RSA. Patrick can usually be found in the Car Hacking or Aerospace village where he volunteered for several years. His passion is embedded systems security and has released research in Avionics, embedded systems and even bricked his own Tesla while trying to make it faster.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA)
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-02 - Map

Description:

The S.O.D.A. Machine Experience:

Imagine being at DEF CON, eager to dive into some serious hacking without being tethered to your laptop. The Shell On Demand Appliance is here to enhance your experience by providing access to anonymous virtual machine using cold hard cash.

What is the Shell On Demand Appliance?

The S.O.D.A. machine is now located in the contest area at the DEF CON Scavenger Hunt booth, offering virtual machines accessible via the DEF CON network. A blend of hardware, software, art, and hacking, using recycled materials to create a sustainable tech experience. The built-in datacenter connects directly to the DEF CON network. Insert cash or coins into the machine to get started, the system deploys the VM to the network, and a receipt with your login credentials is printed. Users receive login credentials to access their virtual machine via remote shell. You can change the password, install tools and applications, and customize the VM to suit your needs. The updated system now provides secure access from anywhere in the world through a web browser or standard SSH client. Be sure to check out the BBS too!

Supporting the Cause:

All proceeds from the S.O.D.A. Machine benefit the National Upcycled Computing Collective, Inc., a 501(c)(3) nonprofit organization dedicated to advancing research and education in computer science, technology, and engineering. Contributions are welcome at https://www.paypal.com/paypalme/NUCC.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA)
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-02 - Map

Description:

The S.O.D.A. Machine Experience:

Imagine being at DEF CON, eager to dive into some serious hacking without being tethered to your laptop. The Shell On Demand Appliance is here to enhance your experience by providing access to anonymous virtual machine using cold hard cash.

What is the Shell On Demand Appliance?

The S.O.D.A. machine is now located in the contest area at the DEF CON Scavenger Hunt booth, offering virtual machines accessible via the DEF CON network. A blend of hardware, software, art, and hacking, using recycled materials to create a sustainable tech experience. The built-in datacenter connects directly to the DEF CON network. Insert cash or coins into the machine to get started, the system deploys the VM to the network, and a receipt with your login credentials is printed. Users receive login credentials to access their virtual machine via remote shell. You can change the password, install tools and applications, and customize the VM to suit your needs. The updated system now provides secure access from anywhere in the world through a web browser or standard SSH client. Be sure to check out the BBS too!

Supporting the Cause:

All proceeds from the S.O.D.A. Machine benefit the National Upcycled Computing Collective, Inc., a 501(c)(3) nonprofit organization dedicated to advancing research and education in computer science, technology, and engineering. Contributions are welcome at https://www.paypal.com/paypalme/NUCC.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA)
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-02 - Map

Description:

The S.O.D.A. Machine Experience:

Imagine being at DEF CON, eager to dive into some serious hacking without being tethered to your laptop. The Shell On Demand Appliance is here to enhance your experience by providing access to anonymous virtual machine using cold hard cash.

What is the Shell On Demand Appliance?

The S.O.D.A. machine is now located in the contest area at the DEF CON Scavenger Hunt booth, offering virtual machines accessible via the DEF CON network. A blend of hardware, software, art, and hacking, using recycled materials to create a sustainable tech experience. The built-in datacenter connects directly to the DEF CON network. Insert cash or coins into the machine to get started, the system deploys the VM to the network, and a receipt with your login credentials is printed. Users receive login credentials to access their virtual machine via remote shell. You can change the password, install tools and applications, and customize the VM to suit your needs. The updated system now provides secure access from anywhere in the world through a web browser or standard SSH client. Be sure to check out the BBS too!

Supporting the Cause:

All proceeds from the S.O.D.A. Machine benefit the National Upcycled Computing Collective, Inc., a 501(c)(3) nonprofit organization dedicated to advancing research and education in computer science, technology, and engineering. Contributions are welcome at https://www.paypal.com/paypalme/NUCC.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 19:35-19:50 PDT

Title: Shifting left in Reversing apk by converting smali to java
When: Saturday, Aug 10, 19:35 - 19:50 PDT
Where: Virtual

Description:
SpeakerBio: Just Tulpa

Hi I'm currently pursuing Msc In Information Security and I'm really interested in Android security

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 11:00-11:45 PDT

Title: SHIM me what you got - Manipulating Shim and Office for Code Injection
When: Saturday, Aug 10, 11:00 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

This talk brings back from the dead an attack surface that security vendors believed they had addressed a long time ago.

We will introduce a novel and stealthy technique to apply malicious shims on a process that does not require registry modification or SDB files and leaves no traces on the disk.

The reverse engineering of the shim infrastructure will be shown while focusing on undocumented API and the kernel driver of the infrastructure.

The various operations offered by the infrastructure will be analyzed from an offensive point of view, and the course we took to achieve this unique technique will be presented.

In addition, we will unveil an attack surface research that resulted in a noteworthy attack that manipulates 2 different OS components into performing DLL injection and privilege escalation.

Researching the undocumented RPC interfaces of the service OfficeClickToRun.exe uncovered a method that can inject a DLL into another process running as “NT AUTHORITY\SYSTEM”, which achieves privilege escalation. For this to work, specific conditions had to be met.

The conditions we tailored will be displayed as we abuse the Opportunistic Lock and App Compatibility (shim) mechanisms.

1. link
2. link
3. link
4. link

Speakers:Ron Ben-Yizhak,David Shandalov

SpeakerBio: Ron Ben-Yizhak, Security Researcher at Deep Instinct

Ron Ben-Yizhak is a security researcher at Deep Instinct.

He is responsible for research of malware campaigns, attack surfaces and vectors and evasion techniques.

His findings are used for developing new analysis, detection, and mitigation capabilities.

Ron joined Deep Instinct in 2019 after serving as a security researcher and forensics specialist in one of the IDF's elite cyber units.

SpeakerBio: David Shandalov, Security Researcher at Deep Instinct

David Shandalov works as a security researcher at Deep Instinct.

His role involves researching and identifying new cyber threats and vulnerabilities, and developing tools for threat detection and analysis.

David began his journey in cybersecurity as a Malware Researcher at Checkpoint and, prior to that, served in the IDF's intelligence corps.

Outside of research, David enjoys flying and is currently working on obtaining his Private Pilot License.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-15:59 PDT

Title: Show & Tell
When: Friday, Aug 9, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Bring a retro artifact of your own for people to have fun with and demonstrate! (Note: Any artifact brought in for Show & Tell must also be taken back home with you, and although we will try our best to keep your artifact safe and operational, we suggest that you don't bring anything irreplaceable or that has sentimental value, as things could get destroyed or go missing.)

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Show & Tell
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Bring a retro artifact of your own for people to have fun with and demonstrate! (Note: Any artifact brought in for Show & Tell must also be taken back home with you, and although we will try our best to keep your artifact safe and operational, we suggest that you don't bring anything irreplaceable or that has sentimental value, as things could get destroyed or go missing.)

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-15:59 PDT

Title: Show & Tell
When: Saturday, Aug 10, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Bring a retro artifact of your own for people to have fun with and demonstrate! (Note: Any artifact brought in for Show & Tell must also be taken back home with you, and although we will try our best to keep your artifact safe and operational, we suggest that you don't bring anything irreplaceable or that has sentimental value, as things could get destroyed or go missing.)

Return to Index - Add to Google - ics Calendar file

XRV - Friday - 10:00-17:59 PDT

Title: Signals Are Everywhere
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

BadVR Data Exploration through VR visualization. See RF signals, cellular signals and step into the data with a hands-on VR experience

Return to Index - Add to Google - ics Calendar file

XRV - Saturday - 10:00-17:59 PDT

Title: Signals Are Everywhere
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

BadVR Data Exploration through VR visualization. See RF signals, cellular signals and step into the data with a hands-on VR experience

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 13:30-14:30 PDT

Title: Signature-Based Detection Using Network Timing
When: Friday, Aug 9, 13:30 - 14:30 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

Malware traffic is commonly identified using signatures based off its code, strings, and associated network infrastructure. However, it's also possible to build signatures from the timing between network transactions. This presentation will explore using network captures of known malicious network activity to find similar behavior in random traffic. The talk is technical as it involves processing packets with Python and a some data science, but will be presented in a way that anyone should be able to understand and enjoy.

SpeakerBio: Josh Pyorre, Security Researcher at Cisco Talos

Josh Pyorre is a Security Researcher with Cisco Talos. He's been in security since 2000 with NASA, Mandiant, and other organizations. Josh has presented at many conferences, such as DEFCON, B-Sides, Derbycon, DeepSec, Qubit, and others. His professional interests involve network, computer and data security with a goal of maintaining and improving the security of as many systems and networks as possible. He's writes dark electronic music under the name Die Vortex.

Return to Index - Add to Google - ics Calendar file

TCV - Friday - 17:00-17:59 PDT

Title: SIMply Secure
When: Friday, Aug 9, 17:00 - 17:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

Join us at Telecom Village, DEFCON for the SIM Card Testing Workshop. We'll cover SIM card functionality, communication protocols, reading and writing techniques, and introduce SIM card algorithms and authentication. Explore emerging eSIM technology and its communication methods. This hands-on workshop equips participants with practical skills in testing and manipulating SIM cards, providing a comprehensive understanding of both traditional SIM and eSIM technologies

SpeakerBio: Zibran Sayyed

Seasoned professional with extensive experience in RAN, VoLTE, and VoWiFi security assessment, demonstrating expertise in safeguarding telecommunications networks. Proficient in a wide range of technologies, including GSM, UMTS, LTE, VoLTE, and 5G.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 13:00-13:50 PDT

Title: Simulated Drone Hacking
When: Friday, Aug 9, 13:00 - 13:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Drone hacking tends to be an expensive and sometimes unsafe, but not if you use a simulator!. I have developed a drone hacking simulator called the Damn Vulnerable Drone.

The Damn Vulnerable Drone is a virtually simulated environment designed for offensive security professionals to safely learn and practice drone hacking techniques. It simulates real-world ArduPilot & MAVLink drone architectures and vulnerabilities, offering a hands-on experience in exploiting drone systems.

SpeakerBio: Nick Aleks
No BIO available

Return to Index - Add to Google - ics Calendar file

PLV - Friday - 17:00-17:45 PDT

Title: Singapore - Safeguarding the Nation: The Vital Role of Cybersecurity in AI-Driven Homeland Security
When: Friday, Aug 9, 17:00 - 17:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

Homeland security agencies have been rapidly developing AI-powered solutions to enhance their operational effectiveness. As AI-powered systems become more ubiquitous, a greater emphasis must be placed on Cybersecurity. A career police officer, Yeow Boon understands first-hand the myriad ways AI can augment Homeland Security operations. In his current roles as the Deputy Chief Executive (Development) and Chief Information Officer of Singapore's Home Team Science and Technology Agency (HTX), Yeow Boon oversees the agency's transformation, and by extension, the AI transformation of Singapore's Home Team. Concurrently, he has to ensure that any risks involved in the increased attack surface associated with the development of AI-powered technologies are mitigated. In his speech, Yeow Boon will highlight the critical role of Cybersecurity in AI-driven homeland security. From the development stage to organisational best practices, he emphasises the importance of keeping Cybersecurity at the forefront of any agency's AI transformation. During this session, look forward to gaining insights into the latest Cybersecurity threats in AI-driven Homeland Security and how to combat them.

Speakers:NG Yeow Boon,Bill Woodcock

SpeakerBio: NG Yeow Boon, Singapore's Home Team Science and Technology Agency
No BIO available
SpeakerBio: Bill Woodcock, Executive Director at Packet Clearing House

Bill Woodcock is the executive director of Packet Clearing House, the intergovernmental treaty organization that supports the operation of critical Internet infrastructure, including Internet exchange points and the core of the domain name system. Since entering the Internet industry in 1985, Bill has helped establish more than three hundred Internet exchange points. In 1989, Bill developed the anycast routing technique that now protects the domain name system. In 1998 he was one of the principal drivers of California 17538.4, the world's first anti-spam legislation. Bill was principal author of the Multicast DNS and Operator Requirements of Infrastructure Management Methods IETF drafts. In 2002 he co-founded INOC-DBA, the security-coordination hotline system that interconnects the network operations centers of more than three thousand Internet Service Providers and Security Operations Centers around the world. And in 2007, Bill was one of the two international liaisons deployed by NSP-Sec to the Estonian CERT during the Russian cyber-attack. In 2011, Bill authored the first survey of Internet interconnection agreements, as input to the OECD's analysis of the Internet economy. Bill served on the Global Commission on the Stability of Cyberspace and on the Commission on Caribbean Communications Resilience. He's on the board of directors of the M3AA Foundation, and was on the board of the American Registry for Internet Numbers for fifteen years. Now, Bill's work focuses principally on the security and economic stability of critical Internet infrastructure.

Return to Index - Add to Google - ics Calendar file

VMV - Friday - 10:00-12:59 PDT

Title: SIV Internet Voting Hacking Challenge
When: Friday, Aug 9, 10:00 - 12:59 PDT
Where: Virtual

Description:

Experts have long agreed that secure internet voting in public elections is not feasible with today's technology, nor with any technologies of the foreseeable future. The challenges are numerous, including many fundamental threats such as vulnerability to malicious clients, authentication attacks, privacy attacks, network and Internet infrastructure attacks, server penetration attacks, and various kinds of denial of service attacks. Internet voting systems also suffer from a lack of any meaningful end-to-end auditability. In this hacking challenge, we will set aside these broader concerns to focus on a specific proposed internet voting system called SIV (Secure Internet Voting) intended for real public elections in the United States. They are conducting a mock online election this week with the specific goal of challenging anyone to break their system.

SpeakerBio: SIV

No BIO available

Return to Index - Add to Google - ics Calendar file

DL - Friday - 12:00-13:45 PDT

Title: Skynet
When: Friday, Aug 9, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W306 - Map

Description:

Skynet is an AI project (just kidding.) It is meant to be a sort of unified theory of detection, enabling us to plot any detection artifact types on screen around an entity and decision them faster and more accurately. While plotting alert sets, attack trees, and kill chains has been done, for the presentation of alert sets and cases, we are planning to use graphing as the primary presentation, triage and decisioning mechanism, at scale, using a novel combination of heuristics and machine learning. It is an alert manager made by users, for users.

Speakers: Craig Chamberlain,Rewanth Tammana

SpeakerBio: Craig Chamberlain

Craig Chamberlain has been working on threat hunting and detection for most of his life and has contributed to several SIEM-like products you may have used. Most of them had unnecessarily simple alert pages and workflow, which makes him sad, and this is his attempt to put things right. He has presented at numerous conferences including the SANS Threat Hunting Summit; RSA 2024; CactusCon; the ISC2 Congress; SOURCE Boston; and several B-Sides conferences in Washington DC, San Francisco, NoVA, Boston, and Rochester.

SpeakerBio: Rewanth Tammana

Rewanth Tammana is a security ninja, open-source contributor, and an independent consultant. Previously, Senior Security Architect at Emirates NBD National Bank of Dubai). He is passionate about DevSecOps, Cloud, and Container Security. He added 17,000+ lines of code to Nmap. Rewanth speaks and delivers training at numerous security conferences worldwide. He was recognized as one of the MVP researchers on Bugcrowd (2018), published an IEEE research paper on ML and security, and more.

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 13:30-13:59 PDT

Title: Small Satellite Modeling and Defender Software
When: Saturday, Aug 10, 13:30 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

The proliferation of ride-share rocket launches and decrease in the overall cost of sending payloads to space due to recent successes in the private space industry has made small satellite systems a cost effective and time-efficient method to put research vehicles in space.

The University of Alabama in Huntsville's Center for Cybersecurity Research and Education (CCRE) has been funded by the U.S. Army Space and Missile Defense Command (SMDC) over the last several years to investigate the overall cybersecurity posture of small satellite systems. Numerous iterations of student teams led by CCRE and SMDC staff members have managed to accomplish notable research milestones.

This talk is meant to inform the next generation in aerospace cybersecurity by discussing our major research milestones, relevant findings, lessons learned, and areas of concern relating to the overall cybersecurity posture of small satellite systems.

Relevant items to be covered in this talk include what it took to build a working small satellite system model as close to real-world as possible (Raspberry Pis vs PyCubed boards vs other contenders), implementation of small satellite functions (payload camera, radio communications, positioning/sensor array, orbital simulation, battery/solar charging, etc.), performing vulnerability analysis against the implemented model, creating different attack scenarios (MitM, DoS, spoofing, hardware attacks), implementing defensive mitigations (hardening scripts, command validation, health checks), and the development of a lightweight software solution named "Small Satellite Defender" (SSD) designed to protect satellites from potential threat vectors.

SpeakerBio: Kyle Murbach, Principal Research Engineer, Center for Cybersecurity Research and Education (UAH/CCRE) at University of Alabama in Huntsville

Dr. Kyle Murbach is a Principal Research Engineer at the University of Alabama in Huntsville's Center for Cybersecurity Research and Education (UAH/CCRE). With over 9 years of experience as a cybersecurity researcher and software reverse engineer with industry and government, he is responsible for leading numerous cybersecurity related projects as PI, Co-PI, and Subject Matter Expert in various topic areas related to malware analysis, tool development, reverse engineering, vulnerability analysis, and computer network operations.

At UAH/CCRE, Dr. Murbach is the technical director for the Space Testing and Resiliency Simulation (STARS) Team where he has led numerous students in the design and development of a small satellite testbed and vulnerability analysis of small satellite systems over the last four years. Dr. Murbach has also led technical development efforts to create an automated malware analysis platform which integrates open-source tools to create high confidence summary information of potential malicious activity in binary files. He also played a key role in the development of a testbed for analysis of malware on non-x86 architectures using emulation and integrated open-source tools to collect comprehensive system data during execution and create visualizations that display potential indicators of compromise to the user. He has worked with private industry partners to assess, reverse engineer, and identify any potential vulnerabilities in a custom cryptographic software.

Dr. Murbach is CISSP certified, he holds his PhD in Cyber Operations from Dakota State University (2019) and BS/MS degrees in Computing Security from Rochester Institute of Technology (2016) as a CyberCorps Scholarship for Service graduate. He has also taught software reverse engineering as an adjunct lecturer for the University of Colorado at Boulder for the last three years.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Small scale LAN party
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Small scale LAN party - Use one of our Windows 98 laptops or BYOB and hook it up! Seating will likely be limited depending on interest.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-15:59 PDT

Title: Small scale LAN party
When: Friday, Aug 9, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Small scale LAN party - Use one of our Windows 98 laptops or BYOB and hook it up! Seating will likely be limited depending on interest.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-15:59 PDT

Title: Small scale LAN party
When: Saturday, Aug 10, 10:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-04-01 - Map

Description:

Small scale LAN party - Use one of our Windows 98 laptops or BYOB and hook it up! Seating will likely be limited depending on interest.

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 13:00-13:30 PDT

Title: Smart Shopping Cart Wheels - How they Work
When: Saturday, Aug 10, 13:00 - 13:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

This talk covers the systems used to physically restrict the motion of shopping carts by locking one or more of their wheels. Topics cover what they are, how they work, and methods to bypass them.

SpeakerBio: Joseph

Joseph is a robotics engineer turned hacker, who takes apart smart shopping cart wheels to see how they work.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 10:30-11:15 PDT

Title: Smishing Smackdown: Unraveling the Threads of USPS Smishing and Fighting Back
When: Saturday, Aug 10, 10:30 - 11:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

It's the holiday season and all through the air,

Messages arrive, not with joy, but despair.

A sinister plot unfolds, a digital dance,

Smishing scammers striking, a threat to enhance.

This past holiday season saw a dramatic rise in SMS phishing (smishing) messages, specifically targeting people pretending to be the USPS. Almost everyone in the United States received one of these messages using a kit sold by the 'Smishing Triad'. While many of us knew these were scams many more did not, including someone close to me.

I knew I had to do something about it once I started receiving these texts myself. With my focus in web application testing, I immediately took interest in these smishing kits and how I could exploit them. After a thorough review, some collaboration with other researchers, and a little reverse engineering I was able to find two vulnerabilities in the scammer's kits allowing me to login to the admin panels.

Using this I have been able to recover over 390k distinct credit cards that the scammers had gathered using over 40 admin panels and well over 900 unique domains. Along with this was info on the scammers themselves like login IPs, usernames, and some cracked passwords they use.

This talk will cover the technical details of how I reverse engineered this kit, found these vulnerabilities, and collected the victim and admin data for each of these sites.

My Blog:

link link

SpeakerBio: S1nn3r

S1nn3r is a recent college graduate. He holds the OSCP, GCIH, eCPPT, Sec+, and some more alphabet soup. He has interned with multiple DoD agencies and now will work in the private sector doing red teaming. During his internships he has worked in exploit development, red teaming, and threat analysis. During his time at school, he has been elected president of the Cybersecurity Club, led multiple CTF teams, organized CTFs, discovered a CVE, and has been awarded over $10k from bug bounty programs.

Return to Index - Add to Google - ics Calendar file

AIxCC - Friday - 11:30-11:50 PDT

Title: SMOKE: Signature Management using Operational Knowledge and Environments
When: Friday, Aug 9, 11:30 - 11:50 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Learn how DARPA's Signature Management using Operational Knowledge and Environments (SMOKE) program aims to develop data-driven tools to automate the planning and execution of emulated threat actor infrastructure needed for red team operations.

SpeakerBio: Tejas Patel, Program Manager at Defense Advanced Research Projects Agency (DARPA)

Hacker Turned Program Manager! Don’t hold it against me!

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 10:00-10:30 PDT

Title: Sneaky Extensions: The MV3 Escape Artists
When: Saturday, Aug 10, 10:00 - 10:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Ever since the pandemic and the rising popularity of work-from-home and hybrid models, there has been an increase in the usage of browsers, particularly video conferencing and collaboration applications. While some extensions enhance the user experience, some can gravely affect users' privacy and security.

Over the past few years, extensions have gained recognition for nefarious activities, from simple color picker extensions to productivity-first AI extensions. And now more than ever, attackers are leveraging malicious extensions to steal user data, promote ads, affiliate marketing, and more. Realizing the abuse, Google pivoted from the MV2 model to the latest MV3, providing better security and locking down the extension from running rampant. While some security measures have been introduced in MV3, it is far from safe. In this talk, we will be demonstrating a suite of attacks, while requiring the least amount of permissions, which 95% of extensions on the Chrome store have. We will showcase stealth stealing of webcam feed, audio streams, clipboard data, and stealing credentials from other extensions like password managers.

MV3 also introduced security measures to block the usage of functions like eval and new Function that allowed arbitrary code execution. We'll showcase how an extension can still do arbitrary code execution effectively bypassing the MV3 restrictions.

In this talk, we will also propose changes to the extension security model to prevent the lurking loopholes. We will also be demonstrating how malicious extensions can interfere with other extensions and steal sensitive information such as Credit card, passwords, OTP, etc, from other extensions.

Speakers: Vivek Ramachandran,Shourya Pratap Singh

SpeakerBio: Vivek Ramachandran, Founder at SquareX

Vivek Ramachandran is a security researcher, book author, speaker-trainer, and serial entrepreneur with over two decades of experience in offensive cybersecurity. He is currently the founder of SquareX, building a browser-native security product focused on detecting, mitigating, and threat-hunting web attacks against enterprise users and consumers. Prior to that, he was the founder of Pentester Academy (acquired in 2021), which has trained thousands of customers from government agencies, Fortune 500 companies, and enterprises from over 140+ countries. Before that, Vivek's company built an 802.11ac monitoring product sold exclusively to defense agencies. Vivek discovered the Caffe Latte attack, broke WEP Cloaking, conceptualized enterprise Wi-Fi Backdoors, and created Chellam (Wi-Fi Firewall), WiMonitor Enterprise (802.11ac monitoring), Chigula (Wi-Fi traffic analysis via SQL), Deceptacon (IoT Honeypots), among others. He is the author of multiple five-star-rated books in offensive cybersecurity, which have sold thousands of copies worldwide and have been translated into multiple languages. He has been a speaker/trainer at top security conferences such as Blackhat USA, Europe and Abu Dhabi, DEFCON, Nullcon, Brucon, HITB, Hacktivity, and others. Vivek's work in cybersecurity has been covered in Forbes, TechCrunch, and other popular media outlets. In a past life, he was one of the programmers of the 802.1x protocol and Port Security in Cisco's 6500 Catalyst series of switches. He was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. He has also published multiple research papers in the field of DDoS, ARP Spoofing Detection, and Anomaly-based Intrusion Detection Systems. In 2021, he was awarded an honorary title of Regional Director of Cybersecurity by Microsoft for a period of three years, and in 2024 he joined the BlackHat Arsenal Review Board.

SpeakerBio: Shourya Pratap Singh, Principal Software Engineer at SquareX

Shourya Pratap Singh is a Principal Software Engineer at SquareX. He is responsible for building SquareX's security-focused extension and works on researching methods to counteract web security risks. He has conducted a workshop at the Texas

Cyber Summit and published work at Blackhat Arsenal EU. He has a bachelor's degree from IIIT Bhubaneswar and holds a patent. His area of interest includes browser extensions and web application security.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 16:30-17:30 PDT

Title: So you wanna know how to make badges
When: Friday, Aug 9, 16:30 - 17:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Taking attendees through the full badge making process from ideation to ordering and producing at scale

SpeakerBio: c0ldbru

No BIO available

Return to Index - Add to Google - ics Calendar file

SEV - Saturday - 10:00-17:59 PDT

Title: Social Engineering Community Village Hours
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Come check out the Social Engineering Community Village!

Return to Index - Add to Google - ics Calendar file

SEV - Sunday - 10:00-13:59 PDT

Title: Social Engineering Community Village Hours
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Come check out the Social Engineering Community Village!

Return to Index - Add to Google - ics Calendar file

SEV - Friday - 08:30-17:59 PDT

Title: Social Engineering Community Village Hours
When: Friday, Aug 9, 08:30 - 17:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Come check out the Social Engineering Community Village!

Return to Index - Add to Google - ics Calendar file

CON - Friday - 09:00-16:59 PDT

Title: Social Engineering Community Vishing Competition (SECVC)
When: Friday, Aug 9, 09:00 - 16:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

In the Social Engineering Community's Vishing Competition (#SECVC), teams and individuals go toe to toe, placing live phone calls in front of the SEC audience at DEF CON, showcasing the duality of ease and complexity of the craft against the various levels of preparedness and defenses by actual companies.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Social Engineering Community Youth Challenge
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Don’t Panic! The Social Engineering Community needs your help save the galaxy! We need brave and creative minds for our Youth Challenge to help us solve a series of challenges that will trigger the implosion failsafe.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 09:00-17:59 PDT

Title: Social Engineering Community Youth Challenge
When: Friday, Aug 9, 09:00 - 17:59 PDT
Where: LVCC West/Floor 3/W317-W319 - Map

Description:

Don’t Panic! The Social Engineering Community needs your help save the galaxy! We need brave and creative minds for our Youth Challenge to help us solve a series of challenges that will trigger the implosion failsafe.

Return to Index - Add to Google - ics Calendar file

PSV - Saturday - 11:00-12:59 PDT

Title: Social Engineering Improv Acting Techniques
When: Saturday, Aug 10, 11:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Social Engineering is a widely-covered topic. We'll focus on how it can be beneficial specifically during covert entry assessments for talking your way in/out of situations as well as to solicit information that you can apply throughout the assessment.

Introductory methods to modern covert entry Tactics, Techniques and Procedures (TTPs) for penetration testers.

An introduction to common and uncommon covert entry techniques that are used during physical security assessments. Whether you are a penetration tester, security coordinator, or the decision maker, these techniques will provide an insight into how expensive electronic and physical access controls can sometimes be bypassed by something as simple as a can of air, a piece of plastic, or even a smile.

Tim Roberts and Brent White of WeHackPeople.com and Dark Wolf Solutions, LLC will be sharing their experiences with covert and overt security tests over the years and walking participants through some real-life application of the techniques utilized during these assessments.

SpeakerBio: Tim Roberts, Covert Entry Specialist at Dark Wolf Solutions

Tim is a Covert Entry Specialist with Dark Wolf Solutions and Sr. Principal Penetration Tester. He is the founding member of the Lexington DEF CON group (DC859). He has been interviewed on the subject of “White hat hacking” for Microsoft’s “Roadtrip Nation” television series, was featured on IDG Enterprise’s CSO Online publication by Ryan Francis on social engineering, and was interviewed at Black Hat by HelpNetSecurity on security awareness and “Know Your Adversary”. He and Brent White have also been featured a couple of times on the true crime series Profiling Evil with Mike King. Tim has over fifteen years of professional security experience and has held management, IT, and physical security roles across multiple industries, including healthcare, finance, and government. His experience includes Red Team, Internal/External Network, Wireless, Application, Physical Security, Social Engineering, and more. Tim has spoken and conducted training at numerous security and hacker conferences, including ISSA International, DEF CON, DerbyCon, NolaCon, various B-Sides, CircleCityCon, Techno Security Con, SaintCon, Appalachian Institute of Digital Evidence at Marshall University, Who’s Your Hacker, was keynote for the S&H Law – FBI/Hacker Panel, and more. By continuing to share these experiences, he hopes to further contribute to the InfoSec community and security awareness as a whole.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 15:30-16:15 PDT

Title: Social Engineering Like you're Picard
When: Friday, Aug 9, 15:30 - 16:15 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

AI is transforming social engineering. Using tools like ChatGPT, Gemini, and Copilot, attackers can make phishing and vishing attacks nearly impossible to distinguish from legitimate Interactions. This presentation will demonstrate how virtually anyone with a pulse can now use AI to craft sophisticated phishing sites and conduct vishing operations with unprecedented subtlety and effectiveness. These next-generation techniques are transforming the landscape of social engineering.

You will learn how to replicate these advanced techniques to elevate your own social-engineering game. You will learn how criminals can manipulate AI tools to simulate real-world attacks and gain a deeper insight into their tactics. You'll learn how to use A.I. to enhance how you attack now & ways for it to supplement skills you don't currently have.

You will learn how to leverage these techniques to transform an organization's, traditional, "security awareness" mentality into a "situational awareness" mindset. Using real-world examples, we demonstrate turning potential threats into teachable moments.

This session is essential for anyone looking to harness the power of AI in hacking and Red Teaming. We offer practical skills to engage employees and enhance your approach to social engineering both offensively and defensively. And yes, we do this with a certain theme in mind as I ENGAGE the audience as we boldly go where no Hackers have gone before!

1. link
2. link
3. link
4. link
5. link
6. link
7. link
8. link
9. link
10. link
11. link
12. link
13. link
14. link

SpeakerBio: Jayson E. Street

Jayson E. Street referred to in the past as:

A "notorious hacker" by FOX25 Boston, "World Class Hacker" by National Geographic Breakthrough Series and described as a "paunchy hacker" by Rolling Stone Magazine. He however prefers if people refer to him simply as a Hacker, Helper & Human.

He's a Simulated Adversary for hire. The author of the "Dissecting the hack: Series" (Which has been taught in colleges and Jayson also appears in college text books as well). Also, the DEF CON Groups Global Ambassador. He's spoken at DEF CON, DEF CON China, GRRCon, DerbyCon and at several other 'CONs & colleges on a variety of Information Security subjects. He was also a guest lecturer for the Beijing Institute of Technology for 10 years.

He loves to explore the world & networks as much as he can. He has successfully robbed banks, hotels, government facilities, Biochemical companies, etc. on five continents (Only successfully robbing the wrong bank in Lebanon once all others he was supposed to)!

Jayson is a highly carbonated speaker who has partaken of Pizza from Bulgaria to Brazil & China to The Canary Islands. He does not expect anybody to still be reading this far but if they are please note he was proud to be chosen as one of Time's persons of the year for 2006.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 11:30-12:25 PDT

Title: Software Defined Radio 101: Capturing Your First RFCTF Flag
When: Friday, Aug 9, 11:30 - 12:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

So you just picked up an RTL-SDR? HackRF? Not sure what to do with it or where to get started? This talk is nothing new or ground–breaking, rather a compilation and lessons learned into the world of software defined radios (SDRs), namely to solve challenges for the RF capture the flag. It will cover topics of SDR basics, hardware comparison and capabilities/limitations, software (focusing on Linux-based operating systems), and the tactics, techniques, and procedures to find your first RF CTF flag and get on the scoreboard. By the end, you will have enough tools and knowledge to start hunting for SDR flags in the ongoing capture the flag.

SpeakerBio: bkobe

bkobe is a formally trained electrical engineer who focuses on all things analog/digital circuits to microcontroller/digital signal processors and software defined radios. Background in hardware printed circuit board design, software/firmware development, radios and repeaters (commercial site installation and maintenance), and recently radio mesh networks. Enjoys the camaraderie in this community with common passions, and the sharing of ideas and knowledge. Member of WhatTheFreq! capture the flag team and the Hard Hat Brigade.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 14:00-17:59 PDT

Title: Sold Out - 64-bit Intel Assembly Language Programming for Hackers
When: Thursday, Aug 8, 14:00 - 17:59 PDT
Where: Springhill Suites/Dunes - Map

Description:

Assembly language has a reputation for being intimidating, but once you learn the basics--and know how to read the documentation for the rest--there's nothing you can't follow. There are many interesting fields of study in computer security that depend on the ""closer to the metal"" knowledge you'll gain from learning to code in assembly: - Software reverse engineering - Vulnerability and exploit research - Malware/implant development - Digital forensics ...among others. There is no substitute for the confidence that you gain from being able to research and understand computer systems at lower levels of abstraction. The purpose of this workshop is to introduce Intel x64 assembly language to the attendees. We will be using the Microsoft Macro Assembler, and we will be examining our code step-by-step in the x64dbg debugger. No prior programming experience is required--we will be working on things from first principles. There will be few slides. Concepts will be presented primarily within the x64dbg environment, with a focus on experimentation and using primary documentation. Attendees can follow along with their own laptops and programming environments. We will cover the following topics: - Assembling and linking code - The execution environment of x64 programs - Memory - Registers - A wide variety of instructions - Addressing modes - How to read instruction documentation in the Intel manuals - Moving data around - Stack operations - x64 ABI and calling conventions - Representing data - Integer math - Program flow: conditional execution, loops - Leveraging the Windows API - How to read MSDN articles on Windows API functions - Resources for reference and future learning

SpeakerBio: Wesley McGrew, Senior Cybersecurity Fellow at MartinFederal

Dr. Wesley McGrew directs research, development, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented on topics of penetration testing and malware analysis at DEF CON and Black Hat USA and taught a self-designed course on reverse engineering to students at Mississippi State University, using real-world, high-profile malware samples. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems.

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 09:00-12:59 PDT

Title: Sold Out - Capture the Flag 101
When: Saturday, Aug 10, 09:00 - 12:59 PDT
Where: Springhill Suites/Dunes - Map

Description:

Capture the Flag (CTF) is a competition where teams and individuals compete to solve security challenges. The one that collects most flags the fastest wins the competition (and typically, prizes). CTF-101 is an interactive workshop where we attendees learn about CTF competitions and common security vulnerabilities in a game-like environment. A couple of challenges are presented throughout the session and our hosts walk through how to solve them and provide support as attendees try to solve the challenges during the live hacking part of the workshop. Plus, there's a leaderboard for attendees to track their progress.

SpeakerBio: Micah Silverman, Director of Security Relations at Snyk

Micah is Snyk's Director of Security Relations. With 29 years of Java Experience (yup, that's from the beginning) and 23 years as a security professional Micah's authored numerous articles, co-authored a Java EE book, and spoken at many conferences. He's a maker, who's built full-size MAME arcade cabinets and repaired old electronic games (http://afitnerd.com/2011/10/16/weekend-project-fix-dark-tower/). He brings his love of all things security and Java to a conference near you!

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 14:00-17:59 PDT

Title: Sold Out - Crash Course in Physical Access Control Systems
When: Saturday, Aug 10, 14:00 - 17:59 PDT
Where: Springhill Suites/Dunes - Map

Description:

This Physical Access Control Learning Lab will teach attendees about physical access control and the systems involved. Many of the subjects being taught will be related to their cybersecurity counterparts and lots of focus placed on the why of each concept, not only the fun parts.

Speakers: Lorenzo Pedroncelli,Randy Belbin

SpeakerBio: Lorenzo Pedroncelli, RSA

Lorenzo has been working with technology since childhood, directly out of high school he went to work for the National Laboratories. Lorenzo helped drive a new security initiative for High Performance Computing, eventually moving to another National Laboratory to do the same. After leaving government contracting Lorenzo joined RSA and started his first "official" job in cybersecurity as a consultant for NetWitness helping customers improve their knowledge and use of the SIEM. Most recently Lorenzo switched into supporting RSA's internal security operations, leading the Converged Security team including the Incident Response, Data Security, Cloud Security, and Endpoint Security programs, among others.

SpeakerBio: Randy Belbin, RSA

Randy began his Information Technology and cybersecurity career in the MSP space over a decade ago, before joining RSA as a Sales Engineer in 2016. In the years since, Randy has become an industry expert for Identity and Access Management. In 2022, Randy moved to RSA’s Security and Risk office to lead the identity program at the newly independent RSA. As part of the security team, Randy has been able to broaden his experience and currently assists with physical security, cloud security, and incident response, in addition to his role as the identity guy.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 14:00-17:59 PDT

Title: Sold Out - Dissecting and Defeating Ransomware's Evasion Tactics
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: Springhill Suites/Sands - Map

Description:

Gain a deeper understanding of how ransomware evades analysis and learn how to identify and counter these techniques. This workshop will explore common evasion methods, how they work, and how you can develop the skills to write code that re-enacts these methods. This workshop will begin by showing you how ransomware builders work. How do the builders generate reliable, viable ransomware code? You'll learn! Once built, how do these malicious binaries implement analysis evasion techniques? Which techniques are used often? How do they function? We'll dive into the most prevalent techniques to show you how they work and why. Finally, you will learn how to re-enact some of these techniques along with more advanced methods within your own code. Are you ready to take your reverse engineering and coding skills to the next levels? – Let's do this! And remember: #RansomwareSucks!

Speakers: Aaron Rosenmund,Josh Stroschein,Ryan Chapman

SpeakerBio: Aaron Rosenmund, Senior Director of Content Strategy & Curriculum at Pluralsight

Aaron Rosenmund is the Senior Director of Content Strategy & Curriculum for Pluralsight, where he has also authored over 115 courses and technical labs across offensive and defensive security operations topics. Part time work includes service as an Cyber Warfare Operations office in the Delaware Air National guard, where he has also led a 100+ member red team for the largest cyber exercise in the Nation, Cybershield.

SpeakerBio: Josh Stroschein, Reverse Engineer, FLARE team at Google

Josh is an experienced malware analyst and reverse engineer and has a passion for sharing his knowledge with others. He is a reverse engineer with the FLARE team at Google, where he focuses on tackling the latest threats. Josh is an accomplished trainer, providing training at places such as Ring Zero, BlackHat, Defcon, Toorcon, Hack-In-The-Box, Suricon, and other public and private venues. Josh is also an author on Pluralsight, where he publishes content around malware analysis, RE, and other security topics.

SpeakerBio: Ryan Chapman

Ryan Chapman is the author of SANS' "FOR528: Ransomware and Cyber Extortion" course, teaches SANS' "FOR610: Reverse Engineering Malware" course, works as a threat hunter @ $dayJob, and is an author for Pluralsight. Ryan has a passion for life-long learning, loves to teach people about ransomware-related attacks, and enjoys pulling apart malware.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 09:00-12:59 PDT

Title: Sold Out - Dissecting Malware for Defense - Crafting Custom Yara Rules
When: Thursday, Aug 8, 09:00 - 12:59 PDT
Where: Springhill Suites/Frontier - Map

Description:

Threat actors skillfully deploy malware to evade detection, outmaneuvering traditional security tools. In this workshop, "Dissecting Malware for Defense - Crafting Custom Yara Rules", you'll harness the power of malware analysis and crowdsourced intelligence to build tailored Yara rules. These rules will supercharge your security systems, enabling you to detect emerging threats, enhance threat hunting, and accurately pinpoint malicious activity. This fast-paced course will guide you in mastering static and behavioral detections, empowering you to safeguard your organization. By the end, you'll expertly translate malware analysis insights into high-quality Yara rules, bolstering your defensive arsenal.

Speakers: Francisco Perdomo,Josh Stroschein

SpeakerBio: Francisco Perdomo, Security Engineer, VirusTotal Research Team at Google

Francisco is a skilled security professional with a strong background in detection engineering and a keen interest in reverse engineering. With extensive blue team experience, he currently works as a Security Engineer at Google's VirusTotal Research team where he leverages his operational expertise to investigate malware trends and create insightful technical content. Francisco's background includes roles as a SecOps Engineer and Professor of Computer Security.

SpeakerBio: Josh Stroschein, Reverse Engineer, FLARE team at Google

Josh is an experienced malware analyst and reverse engineer and has a passion for sharing his knowledge with others. He is a reverse engineer with the FLARE team at Google, where he focuses on tackling the latest threats. Josh is an accomplished trainer, providing training at places such as Ring Zero, BlackHat, Defcon, Toorcon, Hack-In-The-Box, Suricon, and other public and private venues. Josh is also an author on Pluralsight, where he publishes content around malware analysis, RE, and other security topics.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 14:00-17:59 PDT

Title: Sold Out - Dodging the EDR Bullet: A Workshop on Malware Stealth Tactics
When: Thursday, Aug 8, 14:00 - 17:59 PDT
Where: Springhill Suites/Frontier - Map

Description:

The workshop will walk through a number of state of the art techniques used for detection and will show the process of thinking used to research and develop cutting-edge evasion techniques. We will dive deep into interesting aspects of Windows and AV internals with respect to malware development. The focus will be on the mindset used to defeat security products starting with the analysis of a variety of detection mechanisms and ending with the final development of countermeasures. Moreover, the training will contain a number of live demonstrations to practically show how to apply those concepts and how to integrate them, showing how to develop evasive implants and post-exploitation tools. By altering the fundamental rules of engagement, we can confound EDR systems and reshape their perception of the digital environment. The workshop will dig deep into the internals of certain aspects of AV/EDRs and the Windows operating system to identify the area to exploit to lower the detection rate, it will involve the usage of Visual Studio and debuggers.

Speakers: Dimitri Di Cristofaro,Giorgio "gbyolo" Bernardinetti

SpeakerBio: Dimitri Di Cristofaro, Senior Security Consultant and Researcher at SECFORCE LTD

Dimitri "GlenX" Di Cristofaro is a senior security consultant and researcher at the London office of SECFORCE LTD where he performs Red Teams on a daily basis. The main focus of his research activities is about Red Teaming and in particular on identifying new ways of attacking operating systems and looking for cutting edge techniques to increase stealthiness in strictly monitored environments. He enjoys malware writing and offensive tools development as well as producing electronic music in his free time.

SpeakerBio: Giorgio "gbyolo" Bernardinetti, Lead Researcher, System Securitiy Division at CNIT

Giorgio "gbyolo" Bernardinetti is lead researcher at the System Securitiy division of CNIT. His research activities are geared towards Red Teaming support activities, in particular design and development of advanced evasion techniques in strictly monitored environments, with emphasis on (but not limited to) the Windows OS, both in user-space and kernel-space. He is certified OSCP and OSCE, and enjoys playing electric guitar in his free time.

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 14:00-17:59 PDT

Title: Sold Out - Email Detection Engineering and Threat Hunting
When: Saturday, Aug 10, 14:00 - 17:59 PDT
Where: Springhill Suites/Desert Inn - Map

Description:

Email remains the #1 initial access vector for commodity malware and nation state actors. Historically, tackling email-based threats has been considered the purview of black-box vendor solutions, with defenders having limited scope (or tooling!) to swiftly and effectively respond to emerging attacker activity and novel offensive tradecraft. In this workshop, attendees will be given detailed insight into the latest techniques used to deliver prevalent malware strains, including Pikabot and DarkGate, and will hunt through email data to identify this malicious activity, developing rules to detect and block these attacks. Initially attendees will be introduced to the foundational technologies that enable threat hunting, detection engineering, and response in the email domain, before being given access to the email data of a fictitious company seeded with benign and real-world attack data. Throughout the day, participants will learn to hunt common phishing techniques including: - QR codes - Image-as-content - Drive-by delivery via links and HTML smuggling - Excel attachments with embedded links to SMB shares - ISO attachments - PDF attachments with embedded links to malware (PDF -> URL -> ZIP -> WSF) - VIP impersonations - BEC Attendees will be guided through the rule creation process, utilizing free and open detection engines including Sublime and Yara, and will be introduced to the signals and email attributes that can be used to craft high-fidelity rules, including targeted user groups, sentiment analysis, sender domain age, and attachment analysis. Having completed the workshop, attendees will have a strong understanding of the tools and techniques at their disposal to defend their organizations from all manor of email threats.

Speakers: Alfie Champion,Josh Kamdjou

SpeakerBio: Alfie Champion, Co-founder at DelivrTo

Alfie specialises in the delivery of attack detection and adversary emulation services, actively contributing education content, tooling and blogs to further the industry. He has previously worked with organisations across multiple industry verticals to uplift and validate their detective capability through red or purple team engagements, and now leads the global adversary emulation function at a FTSE 250 company. He has previously spoken at BlackHat USA, RSA and Blue Team Con 2022, among others, and is the co-founder of DelivrTo.

SpeakerBio: Josh Kamdjou, Founder and CEO at Sublime Security

Josh has been doing offensive security-related things for the past 12 years. He's spent most of his professional career breaking into networks via spear-phishing and other methods, and building software for both the public (Department of Defense) and private sectors. Josh is the Founder and CEO of Sublime Security, and in his private life enjoys weight lifting, Martial Arts, soccer, and spending time with his niece and nephew.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 09:00-12:59 PDT

Title: Sold Out - Finding the Needle: An Introduction to Detection Engineering
When: Friday, Aug 9, 09:00 - 12:59 PDT
Where: Springhill Suites/Desert Inn - Map

Description:

As defenders, we are always outnumbered, but we are by no means outmaneuvered. Attackers may hide in the haystack of haystacks, but with scalable detection logic, efficient coding practices, a thorough investigation methodology, and a reasonable corpus of computing, we can still determine which haystack to look within, and subsequently find the needle.

This is often made possible by a detection pipeline. And knowing how detection pipelines work, and the role each component plays, can help us write more efficient, more accurate detections to make life hard for the attacker. By reducing the attacker's window of opportunity, whilst making the subsequent investigation easier for the would-be analyst, we can maintain a strong defensive position, forcing the attacker to burn significantly more resources in an attempt to make progress.

This workshop will run attendees through implementing a simple detection pipeline in code, and some basic detection rules, to understand how to: - Ingest and normalize arbitrary log data, and make such data available for downstream detection rules; - Implement detection logic, to isolate potentially malicious behaviour; - Enrich log data with more context, aiding investigation; and - Draw relationships from individual log entries, to reduce investigative noise.

Attendees should be comfortable with either Python 3 or Golang, including core language syntax and the execution environment of their preferred language.

Speakers:
Kathy Zhu,Troy Defty

SpeakerBio:
Kathy Zhu, Security Engineering Tech Lead at Google

Having worked in the security industry for 8+ years, Kathy is currently a Security Engineering Tech Lead in the detection space at Google. Her interest and experience is in detection engineering and software development. Outside of work, she also enjoys running, the outdoors, and reading.

SpeakerBio:
Troy Defty, Security Engineering Manager

Following over a decade in the UK and Australian InfoSec industries, including an 8-and-a-half year stint in red teaming, Troy jumped the proverbial fence from red to blue, and is currently a Security Engineering Manager at a tech company. His interest and experience is in detection engineering, red teaming, threat modelling, hardware, and assessing ICS environments. Other interests include music, electronics, the outdoors, travel, rugby, CTF, and making piano-related noise.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 14:00-17:59 PDT

Title: Sold Out - Flipping the Coin: Red and Blue Teaming in Windows Environments (++)
When: Thursday, Aug 8, 14:00 - 17:59 PDT
Where: Springhill Suites/Dean Martin - Map

Description:

Red and blue are two sides of the same coin. Offensive and defensive teams deliver the best results when working together; sharing knowledge, ideas, and understanding with each other. And a core part of this information exchange is understanding each respective perspective. This is the overarching theme of the workshop; attackers thinking like defenders, and defenders thinking like attackers.

This workshop is the second version of Flipping the Coin and features upgraded attack paths, and lab environments.

By the end of the workshop, attendees will:

1. Understand and perform common offensive attacks (supported by the Metasploit Framework) against Windows Domains, including:
    - Pass the Hash attacks;
    - gMSA Golden Attack;
    - ADCS abuse;
    - Common tunnelling techniques;
    - PrintSpoofer exploits;
    - LSASS exploitation (using Mimikatz);
    - AD enumeration (using BloodHound);
    - DACL abuse;
    - Kerberos golden tickets; and
    - DLL hijacking.
2. Understand the process of detecting attacks against Windows infrastructure, including how to design and implement their own detection rules based on attendees' previous attacks, using:
    - Sigma/Yara rules.
    - Log ingestion/normalisation platforms, and query engines (e.g. ELK).
3. Understand and appreciate how the actions and processes of red and blue teams are interlinked, for the greater collective good.

Recommended (but not required) prior reading: - https://nooblinux.com/metasploit-tutorial/ - https://posts.specterops.io/introducing-bloodhound-enterprise-attack-path-management-for-everyone-39cfd8d6eb7c - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview - https://socprime.com/blog/sigma-rules-the-beginners-guide/ - https://github.com/socprime/SigmaUI - https://blog.netwrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/ - https://posts.specterops.io/certified-pre-owned-d95910965cd2 - https://www.elastic.co/guide/en/security/current/suspicious-print-spooler-point-and-print-dll.html

Much of the material and core concepts of the workshop remain the same from the DEF CON 31 workshop with some updated topics for DEF CON 32, including an updated environment, and gMSA attacks within the lab.

Speakers: Angus Strom,Troy Defty

SpeakerBio: Angus Strom, Senior Security Engineer

Angus (0x10f2c_) is currently a Senior Security Engineer working at a tech company. He obtained a love for all things computers by scavenging computer parts from local garbage pickups as a kid, and then trying to make them work together without blowing up. Angus eventually realised that a career could be made out of his skills hacking together poorly written LUA code in Garry's mod, and finished a Bachelors in Network Security. In his professional career Angus has 5+ years working in Security Consulting, working across many industries and gaining many shells. More recently Angus has made the move to a security engineer focused role. When not hacking he loves to ski on the little snow that Australia has, and loves to paint small miniatures while listening to Drone Metal.

SpeakerBio: Troy Defty, Security Engineering Manager

Following over a decade in the UK and Australian InfoSec industries, including an 8-and-a-half year stint in red teaming, Troy jumped the proverbial fence from red to blue, and is currently a Security Engineering Manager at a tech company. His interest and experience is in detection engineering, red teaming, threat modelling, hardware, and assessing ICS environments. Other interests include music, electronics, the outdoors, travel, rugby, CTF, and making piano-related noise.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 14:00-17:59 PDT

Title: Sold Out - From an attacker's lair to your home: A practical journey through the world of Malware
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: Springhill Suites/Frontier - Map

Description:

Are you ready to dive deep into the world of malware analysis? Join me for an immersive workshop that will demystify the process of dissecting and analyzing malicious software. Throughout this hands-on session, participants will explore essential techniques and methodologies for uncovering the inner workings of malware and identifying potential threats. During the workshop we will analyze different kinds of malware, from malicious documents, .NET malware and more . Through practical demonstrations attendees will learn how to conduct static and dynamic analysis effectively, gaining valuable insights into malware behaviors and characteristics. Moreover, attendees will gain firsthand experience in executing and analyzing techniques used by attackers, deepening their understanding of how threat actors operate and how to detect and mitigate their malware effectively. By the end of the workshop, attendees will have developed practical skills and techniques for analyzing real-world malware samples, empowering them to defend against evolving cyberthreats effectively.

SpeakerBio: Sebastian Tapia De la torre, Offensive Security Architect

Sebastian's journey into cybersecurity began with a childhood fascination for taking things apart and figuring out how they worked. As he grew older, this curiosity evolved into a passion for hacking and uncovering vulnerabilities in websites and applications, landing him a role in vulnerability management. Eventually, he pivoted into a Security Architect role, where he applied offensive thinking with defensive strategies to advance the security posture of the company he works for. Now an Offensive Security Architect, Sebastian specializes in designing and leading purple team exercises, leveraging real attacker TTPs to test and enhance their security posture effectively.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 14:00-17:59 PDT

Title: Sold Out - Ghidra Analysis & Automation Masterclass
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: Springhill Suites/Dean Martin - Map

Description:

Reverse engineering is done for a variety of reasons, most commonly to analyze malware, when searching for (and when looking to understand) vulnerabilities, or simply because of one's curiosity. The NSA understood this early on and developed a framework to aid them in their reversing endeavors, which they open-sourced in early 2019: Ghidra. Since then, Ghidra has been one of the industry standard tools to analyze files, mainly due to its active development, as well as due to its accessible and versatile nature.

This four-hour workshop primarily focuses on the analyst mindset and fundamental knowledge with regards to reverse engineering, including but not limited to understanding Ghidra's core capabilities such as the disassembly and decompiler views, creating and retyping data structures, writing scripts to extend and automate tasks, and the creation and use of function recognition databases for FunctionID and BSim.

The concepts behind the capabilities of Ghidra are the focus of the theory and during the hands-on exercises, allowing one to transfer the gained knowledge to another tool if so desired. As such, this class is perfect for aspiring and beginning analysts, while also providing background information and additional techniques for intermediate analysts.

The workshop's materials will partially consist of multiple malware samples, the precautions for which will be explained in-detail during the workshop, ensuring the safety and integrity of the systems of the attendees. A laptop with a preinstalled Intel based 64-bit Ubuntu 22.04 VM, along with Ghidra, Eclipse, and OpenJDK 21 is required.

Additionally, knowing how to read C/C++ is required when dealing with decompiled code. Being able to read and write Java is required for the automation scripting, even though Python 2 can be used as well. If you cannot write Java and would still like to participate, you are welcome, but do note that this will impede some parts of the workshop's exercises.

SpeakerBio: Max "Libra" Kersten

Max Kersten is a malware analyst, blogger, and speaker who aims to make malware analysis more approachable for those who are starting. In 2019, Max graduated cum laude with a bachelor's in IT & Cyber Security, during which Max also worked as an Android malware analyst. Currently, Max works as a malware analyst at Trellix, where he analyses APT malware and creates open-source tooling to aid such research. Over the past few years, Max spoke at international conferences, such as DEFCON, Black Hat (USA, EU, MEA, Asia), Botconf, Confidence-Conference, HackYeahPL, and HackFestCA. Additionally, he gave guest lectures and workshops for DEFCON, Botconf, several universities, and private entities.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 14:00-17:59 PDT

Title: Sold Out - Hack the connected plant!
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: Springhill Suites/Dunes - Map

Description:

Tired of legacy ICS systems? Attend this workshop to hack the next generation of Industrial Control Systems! No more Modbus, no more standard PLC, no more Purdue model! This workshop is designed to show what the future might look like for Industrial Control Systems, and how it will impact cybersecurity. We'll bring a realistic ICS setup that features all the fancy current and future trends: SD-WAN and Zero Trust, OPC-UA, MQTT, Digital Twin, Edge devices and soft-PLCs to control a small-scale industrial process simulation. After a short introduction, we'll get into hacking! We will walk you through a CTF-style exercise to go from 0 to full industrial process hacking! The CTF will be guided so that everyone learns something and gets a chance to get most flags!

Speakers: Alexandrine Torrents,Arnaud Soullié

SpeakerBio: Alexandrine Torrents, Cybersecurity Expert at Wavestone

Alexandrine Torrents is a cybersecurity expert at Wavestone. She started as a penetration tester, and performed several cybersecurity assessments on ICS. She worked on a few ICS models to demonstrate attacks on PLCs and developed a particular tool to request Siemens PLCs. Then, she started working at securing ICS, especially in the scope of the French military law, helping companies offering a vital service to the nation to comply with security rules. Now, Alexandrine works with different industrial CISOs on their cybersecurity projects: defining secure architectures, hardening systems, implementing detection mechanisms. She is also IEC 62443 certified and still performs assessments on multiple environments.

SpeakerBio: Arnaud Soullié, Senior Manager at Wavestone

Arnaud Soullié (@arnaudsoullie) is a Senior Manager at Wavestone, a global consulting company. For 14 years, he has been performing security assessments and pentests on all types of targets. He started specializing in ICS cybersecurity 10 years ago. He spoke and taught workshops at numerous security conferences on ICS topics : BlackHat Europe, BruCon, CS3STHLM, BSides Las Vegas, DEFCON... He is also the creator of the DYODE project, an open−source data diode aimed at ICS. He has been teaching ICS cybersecurity training since 2015

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 09:00-12:59 PDT

Title: Sold Out - Hacking Apps on Salesforce
When: Saturday, Aug 10, 09:00 - 12:59 PDT
Where: Springhill Suites/Frontier - Map

Description:

This training will cover how to discover vulnerabilities in custom Salesforce applications hosted on the Salesforce PaaS platform. This is not hacking Salesforce itself, but instead custom applications deployed by customers of Salesforce. You should already know OWASP Top 10 fundamentals such as how XSS or injection attacks work. You will learn how to find vulnerabilities specific to Salesforce apps such as SOQL injection, SOSL, cross-site scripting filter bypasses, and bypassing access controls of hidden functions to exfiltrate data. A new open-source tool “PaaS Cloud Goat” will be used to provide a simulated vulnerable Salesforce application for testing. Students will be expected to use a MitM proxy tool (Burp Suite) to craft malicious attacks to exploit the application. This training will provide a lab manual and live walk-through of the attack process and methods. We will also cover source code review and practice how to find vulnerabilities in code and translate them to working exploits of the simulator app.

Takeaways: 1. Hands-on learning opportunity of pen testing custom Salesforce applications 2. Detailed training documentation material about the underlying flaws 3. Consolidated list of common Salesforce application vulnerabilities

SpeakerBio: Rodney David Beede, Principal Consultant

Rodney is a principal consultant and has specialized in web and cloud security for over 10 years. He has spoken at multiple conferences on topics from cloud security engineering to IoT device hacking. He has multiple CVEs for discovered web application security vulnerabilities. He started his career in enterprise web application software development but shifted to the security industry with his master's thesis research project "A Framework for Benevolent Computer Worms" 2012.

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 09:00-12:59 PDT

Title: Sold Out - Hacking The Metal: A Spark of Intelligence
When: Saturday, Aug 10, 09:00 - 12:59 PDT
Where: Springhill Suites/Desert Inn - Map

Description:

We live in a time of unexpected transformation. Machines can hold conversations, compose prose and poetry, and generate very convincing deepfakes. The field of AI where this all happens – deep learning – has a long history, starting with one simple building block: the neural network. In this workshop, we will tour through the evolution of neural networks and discover that much of their evolution occurred in the world of low-level programming. Using C, C++ and a bit of assembly language, we will learn the fundamentals behind neural networks in their various forms, and build a foundation of knowledge that will allow us to understand how we arrived at large language models, the current state of the art. Most importantly, we will discover how far we can stretch everyday hardware to run deep learning models that solve interesting problems.

SpeakerBio: eigentourist

Eigentourist is a programmer who learned the craft in the early 1980s. He began formal education in computer science when the height of software engineering discipline meant avoiding the use of GOTO statements. Over the course of his career, he has created code of beautiful simplicity and elegance, and of horrific complexity and unpredictability. Sometimes, it's hard to tell which was which. Today, he works on systems integration and engineering in the healthcare industry.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 14:00-17:59 PDT

Title: Sold Out - Hide your kids, turn off your Wi-Fi, they Rogue APing up in here; 201
When: Thursday, Aug 8, 14:00 - 17:59 PDT
Where: Springhill Suites/Sands - Map

Description:

In the 201 version of Hide your kids, turn off your Wi-Fi, they Rogue APing up in here, we will launch the next level of attacks using Rogue APs and other wireless tools. We will look into different ways to attack wireless networks and leverage credentials harvested to gain a foothold, PITM, deliver payloads, and demonstrate impact to the client. During the workshop we will walk through different attacks against OPEN, WPA2, and 802.1X networks. During the CTF participants will have the chance to attack a simulated client network to leverage the attacks learned during the workshop. We will be using EAPHAMMER, BERATE_AP, WIFIPUMPKIN3, BETTERCAP, and RESPONDER. This workshop will be at the Intermediate level(all skill levels welcome), participants should have a solid knowledge of Linux, 802.11, networking, and using virtual machines. It is recommended that all students use the provided VM.

SpeakerBio: James Hawk, Senior Consultant, Proactive Services at Google Public Sector

James Hawk (He/Him) is a Senior Consultant with Google Public Sector, within Proactive Services. He is the wireless subject matter expert for his team. James has led and contributed to multiple assessments (Red Teams and Pen Tests). He has developed internal training and tool updates for 802.11 for his company and team. James is a 20-year veteran of the U.S. Army and has over 10 years of hands-on experience in wireless technologies. James is always researching/testing 802.11 attacks against his home lab. He is a fan of hockey, Letter Kenny, and almost anything Sci-Fi.

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 09:00-12:59 PDT

Title: Sold Out - Industrial Control Systems: how to secure them in practice!
When: Saturday, Aug 10, 09:00 - 12:59 PDT
Where: Springhill Suites/Sands - Map

Description:

"Pentesting ICS is too easy and you are looking for a new challenge? Attend this workshop to discover and practice how to secure Industrial Control Systems! This workshop is designed to show some key cybersecurity measures to implement on Industrial Control Systems. We'll bring a realistic but simple ICS setup and let you secure it step by step. After a short introduction, we'll deep dive in several hands-on exercises: ICS inventory, backups, network security, system hardening and detection. "

SpeakerBio: Alexandrine Torrents, Cybersecurity Expert at Wavestone

Alexandrine Torrents is a cybersecurity expert at Wavestone. She started as a penetration tester, and performed several cybersecurity assessments on ICS. She worked on a few ICS models to demonstrate attacks on PLCs and developed a particular tool to request Siemens PLCs. Then, she started working at securing ICS, especially in the scope of the French military law, helping companies offering a vital service to the nation to comply with security rules. Now, Alexandrine works with different industrial CISOs on their cybersecurity projects: defining secure architectures, hardening systems, implementing detection mechanisms. She is also IEC 62443 certified and still performs assessments on multiple environments.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 14:00-17:59 PDT

Title: Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: Springhill Suites/Desert Inn - Map

Description:

BLE CTF is a series of Bluetooth Low Energy challenges in a capture-the-flag format. It was created to teach the fundamentals of interacting with and hacking Bluetooth Low Energy services. Each exercise, or flag, aims to interactively introduce a new concept to the user. Over the past few years, BLE CTF has expanded to support multiple platforms and skill levels. Various books, workshops, training, and conferences have utilized it as an educational platform and CTF. As an open source, low-cost of entry, and expandable education solution, BLE CTF has helped progress Bluetooth security research. This workshop will teach the fundamentals of interacting with and hacking Bluetooth Low Energy services. Each exercise, or flag, aims to interactively introduce a new concept to the user. For this workshop, we will undergo a series of exercises to teach beginner students new concepts and allow more seasoned users to try new tools and techniques. After completing this workshop, you should have a good solid understanding of how to interact with and hack on BLE devices in the wild. If you have done BLE CTF in the past, this class is still valuable. For advanced users, we offer BLE CTF Infinity, a sequel to BLE CTF. The workshop will also showcase new hardware platforms and client tools for interacting with and completing the exercises. To prepare for the workshop, please follow the setup documentation located at https://github.com/hackgnar/ble_ctf/blob/master/docs/workshop_setup.md

Speakers: Alek Amrani,Ryan Holeman

SpeakerBio: Alek Amrani

Alek Amrani is bad at expense reports.

SpeakerBio: Ryan Holeman, CISO at Stability AI

Ryan Holeman resides in Austin, Texas, where he works as the CISO for Stability AI. He is currently pursuing a Ph.D. in cyber defense from Dakota State University. He has spoken at respected venues such as Black Hat, DEF CON, Lockdown, BSides, Ruxcon, Notacon, and Shmoocon. You can keep up with his current activity, open source contributions, and general news on his blog. His spare time is mostly spent digging into various network protocols, random hacking, creating art, and shredding local skateparks.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 14:00-17:59 PDT

Title: Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming
When: Thursday, Aug 8, 14:00 - 17:59 PDT
Where: Springhill Suites/Desert Inn - Map

Description:

Command and Control (C2) play a crucial role for Red Teams and Advanced Persistent Threats (APTs), establishing persistent access and control over targeted networks. This workshop offers an in-depth exploration of the C2 frameworks, with a specific focus on the open-source Empire framework. Participants will gain valuable insights into the deployment, features, and real-world application of C2 in offensive security. Attendees will learn how to leverage Empire to create, customize, and execute advanced attack scenarios, honing their skills as red team operators. Through practical exercises, attendees will learn to navigate the Empire framework, from basic setup to deploying sophisticated C2 infrastructures. The workshop covers key aspects such as listener configurations, agent management, and the utilization of Empire's diverse modules for effective post-exploitation. A unique feature of this training is the inclusion of a mini Capture-The-Flag (CTF) challenge, offering participants a hands-on opportunity to apply their skills in a controlled, competitive environment. By the conclusion of this workshop, participants will be equipped with the knowledge and skills to leverage the Empire framework effectively in their red team operations, enhancing their capabilities in conducting advanced cyber attacks and navigating the complexities of modern cybersecurity landscapes. Key Workshop Highlights: Comprehensive Introduction to Empire: Gain a solid understanding of Empire's capabilities, setup procedures, and its role in modern offensive operations. Hands-On Deployment and Configuration: Learn through doing, with exercises designed to build proficiency in configuring Empire, managing agents, and customizing listeners. Advanced Attack Scenarios: Delve into sophisticated techniques for post-exploitation, credential harvesting, and evasion, enhancing your arsenal as a red team operator. Real-World Application: Translate workshop learnings into actionable skills through a mini CTF challenge, simulating real-world offensive scenarios in a cloud-hosted environment.

Speakers: Jake “Hubble” Krasnov,Kevin "Kent" Clark,Rey "Privesc" Bango

SpeakerBio: Jake “Hubble” Krasnov, Red Team Operations Lead and Chief Executive Officer at BC Security

Jake "Hubble" Krasnov is the Red Team Operations Lead and Chief Executive Officer of BC Security. He has spent the first half of his career as an Astronautical Engineer overseeing rocket modifications for the Air Force. He then moved into offensive security, running operational cyber testing for fighter aircraft and operating on a red team. Jake has presented at DEF CON, where he taught courses on offensive PowerShell and has been recognized by Microsoft for his discovery of a vulnerability in AMSI. Jake has authored numerous tools, including Invoke-PrintDemon and Invoke-ZeroLogon, and is the co-author of a cybersecurity blog at https://www.bc-security.org/blog/.

SpeakerBio: Kevin "Kent" Clark, Security Consultant at TrustedSec

Kevin "Kent" Clark is a Security Consultant with TrustedSec and a Red Team Instructor with BC Security. His previous work includes Penetration Testing and Red Team Operator, focusing on initial access and active directory exploitation. Kevin contributes to open-source tools such as PowerShell Empire and publishes custom security toolkits such as Badrats and WindowsBinaryReplacements. Kevin authors a cybersecurity blog at https://henpeebin.com/kevin/blog.

SpeakerBio: Rey "Privesc" Bango, Principal Cloud Advocate at Microsoft

Rey "Privesc" Bango is a Principal Cloud Advocate at Microsoft focused on empowering companies and information technologists to take full advantage of transformative technologies. He works to build patterns and practices that streamline the development of solutions that take advantage of Artificial Intelligence and Machine Learning while ensuring that trust and confidence are a top priority, whether through security or responsible use of technology. Since 1989, Rey has explored the world of information technology through the lens of software developer, open-source contributor, cybersecurity practitioner,

and an advocate for the secure and responsible use of artificial intelligence for social good.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 09:00-12:59 PDT

Title: Sold Out - Machine Learning for N00bs
When: Friday, Aug 9, 09:00 - 12:59 PDT
Where: Springhill Suites/Sands - Map

Description:

Every technical product is now incorporating machine learning at an explosive rate. But most people, even those with strong technical skills, don't understand how it works, what its capabilities are, and what security risks come with it. In this workshop, we'll make machine learning models using simple Python scripts, train them, and evaluate their worth. Projects include computer vision, breaking a CAPTCHA, deblurring images, regression, and classification tasks. We will perform poisoning and evasion attacks on machine learning systems, and implement deep neural rejection to block such attacks. No experience with programming or machine learning is required, and the only software required is a Web browser. We will use TensorFlow on free Google Colab cloud systems. All materials and challenges are freely available at samsclass.info, and will remain available after the workshop ends.

Speakers: Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman,Sam Bowne

SpeakerBio: Elizabeth Biddlecome

Elizabeth Biddlecome is a consultant and instructor, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

SpeakerBio: Irvin Lemus, Cyber Range Engineer at By Light IT Professional Services

Irvin Lemus, CISSP is a Cyber Range Engineer at By Light IT Professional Services, training military personnel through international cyber security exercises. Irvin has been in the field since 2006, involved with cybersecurity competitions since 2015 as a trainer, coach, and mentor. He also has taught IT and Cybersecurity courses at Coastline and Cabrillo Colleges. He is the BACCC Cyber Competitions Regional Coordinator, Board member at Pacific Hackers and is a speaker at DEFCON. He describes himself as, "A professional troublemaker who loves hacking all the things."

SpeakerBio: Kaitlyn Handelman, Offensive Security Engineer at Amazon

Kaitlyn Handelman is an offensive security engineer at Amazon. Her focus is cybersecurity in space. In addition to traditional penetration testing, Kaitlyn works on physical devices and RF signals. In her free time, she enjoys ham radio, astronomy, and her cat, Astrocat.

SpeakerBio: Sam Bowne, Instructor at City College San Francisco

Sam Bowne has been teaching computer networking and security classes at City College San Francisco since 2000, and is the founder of Infosec Decoded, Inc. He has given talks and hands-on trainings at Black Hat USA, RSA, DEF CON, DEF CON China, HOPE, and many other conferences. Credentials: PhD, CISSP, DEF CON Black Badge Co-Winner

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 14:00-17:59 PDT

Title: Sold Out - Master Class: Hands-On Machine Learning to Enhance Malware Analysis, Classification, and Detection
When: Saturday, Aug 10, 14:00 - 17:59 PDT
Where: Springhill Suites/Sands - Map

Description:

Malware continues to increase in prevalence and sophistication. VirusTotal reported a daily submission of 2M+ malware samples. Of those 2 million malware daily submissions, over 1 million were unique malware samples. Successfully exploiting networks and systems has become a highly profitable operation for malicious threat actors. Traditional detection mechanisms including antivirus software fail to adequately detect new and varied malware. Artificial Intelligence provides advanced capabilities that can enhance cybersecurity. The purpose of this workshop is to provide an immersive, hands on projects that teach security analysts how to train Machine Learning models to detect thousands and thousands of unique malware samples. This workshop delivers a new framework that uses Machine Learning models to analyze malware, produce uniform datasets for additional analysis, and classify malicious samples into malware families. Additionally, this research presents a new Ensemble Classification Facility we developed that leverages several Machine Learning models to enhance malware classification. To our knowledge, this is the first research that utilizes Machine Learning to provide enhanced classification of an entire 200+ gigabyte-malware family corpus consisting of 80K+ unique malware samples and 70+ unique malware families. New, labeled datasets are released to aid in future classification of malware. It is time we leverage the capabilities of Artificial Intelligence and Machine Learning to enhance detection and classification of malware. Topics taught through hands-on projects include Machine Learning, Natural Language Processing, and Deep Learning models. This workshop provides a pathway to incorporate Artificial Intelligence into the automated malware analysis domain.

SpeakerBio: Solomon Sonya, Computer Science Graduate Student at Purdue University

Solomon Sonya (@0xSolomonSonya) is a Computer Science Graduate Student at Purdue University. He earned his undergraduate degree in Computer Science and Master's Degrees in Computer Science, Information Systems Engineering, and Operational Strategy. Solomon routinely develops new cybersecurity tools and presents research, leads workshops, and delivers keynote addresses at cyber security conferences around the world. Prior to attending Purdue, Solomon was the Director of Cyber Operations Training. Prior to that position, Solomon was a Distinguished Computer Science Instructor at the United States Air Force Academy, Research Scholar at the University of Southern California, Los Angeles, and an Adjunct Faculty Instructor with the Advanced Course in Engineering Cyberspace Security (ACE) at the Air Force Research Lab in Rome, NY.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 09:00-12:59 PDT

Title: Sold Out - Med Team vs Red Team: Intro into Medical Device Hacking
When: Thursday, Aug 8, 09:00 - 12:59 PDT
Where: Springhill Suites/Desert Inn - Map

Description:

Connected medical device and medical device security assessments utilize a varying and wide range of practices, from reverse engineering to hardware exploitation. If you have ever been curious about how to get started, this is the class for you. We will be covering how to get started in Adversarial Medical Device testing, tooling, tactics, exploits and certain bypasses to restrictions you may encounter during testing these devices. Use the tactics learned to exploit devices within the Device Lab!

Speakers: Alex Delifer,Michael "v3ga" Aguilar

SpeakerBio: Alex Delifer

Alex is medical device testing sledgehammer. He is a DevSecOps guru for a large medical device company and cut his teeth building, maintaining and hacking medical devices.

SpeakerBio: Michael "v3ga" Aguilar, Principle Consultant at Secureworks Adversary Group

Michael Aguilar (v3ga) is a Principle Consultant for Secureworks Adversary Group. He runs Adversary Simulation operations, Physical Security and Network/Web based assessments as well as Adversarial Medical Device Tests. When not doing computer things, he reads a lot and likes to run to de-stress. He is also an avid fan of playing guitar really fast and screaming at people.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 09:00-12:59 PDT

Title: Sold Out - Offensive SCCM: Abusing Microsoft's C2 Framework
When: Thursday, Aug 8, 09:00 - 12:59 PDT
Where: Springhill Suites/Dean Martin - Map

Description:

Microsoft Configuration Manager, formerly SCCM (System Center Configuration Manager), is a powerful technology that has been used to deploy software to Windows systems in the majority of enterprise environments since it was released by Microsoft in 1994. Although SCCM has a high potential for abuse due to its privileged access to entire fleets of servers and workstations, it has not been heavily researched or leveraged by security professionals until recently, presumably due to the time-consuming installation process and learning curve. In this workshop, students will be provided access to a live environment that reflects an enterprise SCCM deployment, gain an understanding of how the different components of SCCM interact, and learn how to execute recently discovered attack primitives that can be used compromise SCCM clients, servers, and entire hierarchies. By completing both guided exercises and optional CTF challenges in this lab environment, students will learn how to demonstrate the impact of attack paths involving SCCM.

By the end of this workshop, participants will be able to: - understand the foundational concepts needed to attack and defend SCCM - understand SCCM defaults and configurations that can be abused - use SCCM to complete a realistic attack chain, including recon, privilege escalation, credential gathering, site takeover, and lateral movement - understand how to use offensive security tools to interact with SCCM, such as SCCMHunter, SharpSCCM, sccmwtf, PXEThief, and ntlmrelayx

To get the most out of this training, participants will benefit from reviewing the following resources, although they are not required: - Misconfiguration Manager (misconfigurationmanager.com) - System Center Configuration Manager Current Branch Unleashed, by Kerrie Meyler - Configuration Manager Terminology - Looking Inside Configuration Manager - Network Design - Client Management

This workshop is the second version of Flipping the Coin and features upgraded attack paths, and lab environments.

By the end of the workshop, attendees will:

1. Understand and perform common offensive attacks (supported by the Metasploit Framework) against Windows Domains, including:
    - Pass the Hash attacks;
    - gMSA Golden Attack;
    - ADCS abuse;
    - Common tunnelling techniques;
    - PrintSpoofer exploits;
    - LSASS exploitation (using Mimikatz);
    - AD enumeration (using BloodHound);
    - DACL abuse;
    - Kerberos golden tickets; and
    - DLL hijacking.
2. Understand the process of detecting attacks against Windows infrastructure, including how to design and implement their own detection rules based on attendees' previous attacks, using:
    - Sigma/Yara rules.
    - Log ingestion/normalisation platforms, and query engines (e.g. ELK).
3. Understand and appreciate how the actions and processes of red and blue teams are interlinked, for the greater collective good.

Recommended (but not required) prior reading:

- https://nooblinux.com/metasploit-tutorial/
- https://posts.specterops.io/introducing-bloodhound-enterprise-attack-path-management-for-everyone-39cfd8d6eb7c
- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-ov
- https://socprime.com/blog/sigma-rules-the-beginners-guide/
- https://github.com/socprime/SigmaUI
- https://blog.netwrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/
- https://posts.specterops.io/certified-pre-owned-d95910965cd2
- https://www.elastic.co/guide/en/security/current/suspicious-print-spooler-point-and-print-dll.html

Much of the material and core concepts of the workshop remain the same from the DEF CON 31 workshop with some updated topics for DEF CON 32, including an updated environment, and gMSA attacks within the lab.

Since 2022, Chris, Duane, and Garrett have released a combined 8 blog posts and authored 3 tools (SharpSCCM, SCCMHunter, and Misconfiguration Manager) that demonstrate novel offensive techniques to abuse SCCM functionality.

Speakers: Chris Thompson,Duane Michael,Garrett Foster

SpeakerBio: Chris Thompson, Principal Consultant at SpecterOps

Chris Thompson (@_Mayyhem) is a Principal Consultant at SpecterOps, where he conducts red team operations, research, tool development, and training. Chris has instructed at Black Hat USA/EU and spoken at Arsenal, DEF CON Demo Labs, SO-CON, and Troopers. He is the primary author of Maestro and SharpSCCM and co-author of Misconfiguration Manager, an open-source tool and knowledge base that can be used to help demonstrate, mitigate, and detect attacks that abuse Microsoft Configuration Manager (formerly SCCM).

SpeakerBio: Duane Michael, Managing Consultant at SpecterOps

Duane Michael (@subat0mik) is a Managing Consultant at SpecterOps, where he conducts red team operations, penetration tests, research, course development, and training. Duane has instructed courses on red teaming and vulnerability research at BH USA/EU, NorthSec, and SO-CON. He has presented at Arsenal and DEF CON Demo Labs, contributes to various open source projects, and is a co-author of Misconfiguration Manager.

SpeakerBio: Garrett Foster, Senior Consultant at SpecterOps

Garrett Foster (@garrfoster) is a Senior Consultant at SpecterOps, where he conducts red team operations, penetration testing, research, training, and course development. Garrett has presented at WWHF and BsidesPDX. Garrett is a the primary author of SCCMHunter and a co-author of Misconfiguration Manager.

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 14:00-17:59 PDT

Title: Sold Out - Playing with RFID
When: Saturday, Aug 10, 14:00 - 17:59 PDT
Where: Springhill Suites/Frontier - Map

Description:

Get ready for everything you always wanted to know about RFID, but were afraid to ask! The workshop will start with a basic introduction to Radio-frequency Identification (RFID) and build to a set of practical hands-on challenges. The workshop delves into the theory behind RFID, including different types and protocols (insecure vs. secure types), and how to perform an assessment. Several hands-on assignments will punctuate the theory portion, preparing participants for challenges (of increasing difficulty) on an RFID simulation device, all while participants obtain points for the CTF contest. The objective is to make this workshop fun and accessible to a wide audience. The RFID protocols discussed and in the challenges will be limited to HID and Mifare Classic Instructions and walkthroughs for three devices will be available in the workshop materials, including: * Proxmark3 * Flipper Zero * ACR122U ACR122U devices will be available from the instructor during the workshop.

SpeakerBio: Vinnie "kernelpaniek" Vanhoecke, Senior Security Consultant at Bishop Fox

Vinnie Vanhoecke (OSCE, OSCP) is a Senior Security Consultant at Bishop Fox, where he focuses on web application assessments (static and dynamic), external and internal network penetration testing, and cloud security assessments. He also has extensive experience in red teaming and mobile application assessments for Android. As hobby he likes anything from space to nature, HAM radio, 3D printing and any other IT related topic. Vinnie holds a Bachelor of Computer Science with a Computer and Cybercrime Professional specialisation from Howest in Bruges, Belgium.

Return to Index - Add to Google - ics Calendar file

WS - Saturday - 09:00-12:59 PDT

Title: Sold Out - Sharp Security from All Angles: Mastering Security in .NET Core 8 and Angular 17 Applications
When: Saturday, Aug 10, 09:00 - 12:59 PDT
Where: Springhill Suites/Dean Martin - Map

Description:

We've developed an interactive workshop for all those who want to learn secure coding practices and/or experience attacking with up-to-date technologies. We prefer simplicity: Attacks are performed with swagger and C# scripts, and exploit XSS, CSRF, SSRF, and SQLI. We'll also steal secrets and cookies. Secure coding practices are summarized in an easy-to-remember acronym (PREVENT). Participants will transform RecipeRealm, a naive webapi+angular recipes repository, into a secure solution. Through the hands-on real-world coding exercises, we will cover dealing with a vulnerable third party, using the built-in defense mechanism of Angular, implementing antiCSRF mechanisms, coding a secure data layer, and how to protect a web API from being exploited to get information about our internal assets.

Speakers:Or Sahar,Yariv Tal

SpeakerBio: Or Sahar, Co-founder at Secure From Scratch

Or Sahar is a security researcher and the co-founder of Secure From Scratch. With two decades of experience in software development and security, she specializes in penetration testing, application security, and instructing on secure coding practices. Currently pursuing a second Master's degree in computer science, Or Sahar holds a BSc in software engineering and is certified as an OSCE.

SpeakerBio: Yariv Tal

Yariv Tal is a senior developer turned security researcher. He graduated Summa Cum Laude with a BSc in Software Engineering and is currently pursuing a Master's degree in Computer Science. Yariv leverages his four decades of programming experience, university lecturing, and BootCamp mentoring to promote a "secure from scratch" coding philosophy.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 09:00-12:59 PDT

Title: Sold Out - Small Choices, Global Repercussions: A Tabletop Exercise about Decision-Making in Healthcare Cybersecurity
When: Friday, Aug 9, 09:00 - 12:59 PDT
Where: Springhill Suites/Frontier - Map

Description:

In the unpredictable world of healthcare, the ability to respond effectively to emergencies and technology failures is paramount to ensuring patient safety and continuity of care. As hospitals and emergency rooms increasingly rely on technology to deliver critical services, it's essential for all personnel to understand the complex interplay between technology, emergency response, and the potential cascading effects of failures. This immersive workshop is designed to equip participants with the knowledge and skills needed to navigate emergencies and technology failures in healthcare environments. Through a series of simulated scenarios encompassing various emergency situations and technology breakdowns, participants will explore the intricate challenges of maintaining operational resilience in the face of adversity. From power outages to cyberattacks, participants will learn how to identify, assess, and respond to emergencies with a focus on mitigating second and third-order consequences. Leveraging real-time data and insights from tools and techniques, participants will gain practical experience in detecting anomalies, coordinating response efforts, and minimizing disruption to patient care. Key Learning Objectives: Understand the complex interplay between technology, emergency response, and the potential cascading effects of failures in healthcare environments. Explore various emergency scenarios and technology failures, including power outages, cyberattacks, and system malfunctions. Gain practical experience in assessing the impact of emergencies and technology failures on patient care and operational continuity. Learn how to use the available tools for real-time monitoring, detection, and response to security incidents and technology failures. Discuss strategies for mitigating second and third-order consequences of emergencies and technology failures, including communication, collaboration, and contingency planning.

Speakers: Isabel Straw,Jorge Acevedo Canabal,Nathan Case

SpeakerBio: Isabel Straw, MD

UK Emergency Doctor, Artificial intelligence in Health PHD & Cybersecurity Researcher, Fulbright & Thouron Alum (Global Health Scholar)

SpeakerBio: Jorge Acevedo Canabal, Adjunct Professor at University of Puerto RicoMD

Physician, Adjunct Professor at University of Puerto Rico with Research in Natural Disaster Recovery, Emerging Healthcare Crises, Cyber Resiliency, and Vulnerable Populations (rare genetic disease, extremes of human life-span)

SpeakerBio: Nathan Case

CISO, CTO, Incident Responder, Tinkerer, and Dumpster fire guru

Return to Index - Add to Google - ics Calendar file

Title: Sold Out - Supercharge SAST: Semgrep Strategies for Secure Software
When: Thursday, Aug 8, 09:00 - 12:59 PDT
Where: Springhill Suites/Dunes - Map

Description:

Before the Training: Attendees are expected to have a basic understanding of programming concepts and syntax in a programming language such as JavaScript, Python, Go, or C#/Java. While familiarity with common security vulnerabilities (e.g., OWASP Top 10) is beneficial, it is not a prerequisite.To ensure a smooth and productive experience, participants should come equipped with a laptop that has administrative access for software installation. A pre-training checklist, including software installation guides (Semgrep and a preferred text editor/IDE), will be provided to all registered attendees to prepare them for the workshop.
Participants will: - Gain an understanding of SAST and its importance in the AppSec ecosystem. - Learn to navigate Semgrep's rule syntax and create custom rules tailored to their specific security needs. - Engage in hands-on exercises to apply Semgrep on real-world code snippets and projects, enhancing their learning through practical application. - Explore the Semgrep Playground for testing and refining rules in an interactive environment. - Delve into advanced Semgrep features and techniques for a comprehensive security strategy. - Understand how Semgrep findings can be leveraged for LLM-based code analysis, taking code security to the next level.
Supercharge SAST: Semgrep Strategies for Secure Software" is a meticulously designed workshop aimed at introducing participants to the world of Static Application Security Testing (SAST) through the lens of Semgrep, a cutting-edge tool that combines the simplicity of syntax with the power of complex analysis.
Technical Level and Tools Used: This workshop is tailored for beginner to intermediate skill levels, focusing on practical, actionable insights that participants can immediately apply to their projects. The primary tool used will be Semgrep, supplemented by the Semgrep Playground for online rule testing. Instructions for installing necessary software and accessing online resources will be provided ahead of the workshop.
What You Will Learn: This workshop is structured to guide attendees from the foundational concepts of SAST and application security to the practical application of Semgrep for identifying and mitigating security risks in codebases.

Speakers: Arjun Gopalakrishna,Gautam Peri,Marcelo Ribeiro

SpeakerBio: Arjun Gopalakrishna, Senior Software Security Engineering Manager, Azure Security at Microsoft

Arjun Gopalakrishna is a Senior Software Security Engineering Manager in Azure Security with more than a decade of experience at Microsoft. His work has been instrumental in fortifying Microsoft's Azure platform against a myriad of cyberthreats. His expertise lies in developing and implementing robust security measures to protect cloud-based systems and data. Arjun has presented at DEFCON in 2021, in addition to numerous security talks internally at Microsoft. Arjun's commitment to continuous learning and development, coupled with his passion for cybersecurity, continues to drive his contributions to the field.

SpeakerBio: Gautam Peri, Senior Security Engineer, EPSF SERPENT Team at Microsoft

Gautam Peri is a Senior Security Engineer in EPSF SERPENT (Service Pentest) team at Microsoft. He has over 8 years of experience as a security professional in multiple organizations including Microsoft and Citibank N.A. He started his career as a software developer and became a security professional. Currently, Gautam focuses on securing in Azure Edge & Platform & Devices services at Microsoft. He is passionate about identifying vulnerabilities at scale. Gautam presented at multiple internal events and got accepted to OWASP BASC (Boston Application Security Conference) 2024. Gautam holds CISSP & GCPN certifications, he is committed to continuous learning and development and drives internal knowledge share events.

SpeakerBio: Marcelo Ribeiro, Senior Offensive Security Engineer in Azure Security at Microsoft

Marcelo Ribeiro is a Senior Offensive Security Engineer in Azure Security with over 20 years of experience in various organizations, including Microsoft, IBM, and the Brazilian Navy. As a former Navy Officer, Marcelo was instrumental in

establishing the Brazilian Navy's Cyber Security capacity. He also played a pivotal role in building IBM's DFIR (Digital Forensics and Incident Response) practice in Latin America. Currently, Marcelo focuses on enhancing the security of Microsoft's Azure platform against the constantly evolving cyber threats landscape. Always seeking new challenges, Marcelo's commitment to learning keeps his passion for cybersecurity alive. Marcelo holds several certifications, including CISSP, CISM, OSCP, CEH, GXPN, GPEN, GWAPT, GAWN, GPYC, GREM, GISP, GICSP, GRID, GNFA, GCIH, GCIA, GSEC, and MCSE, among others. In 2023, Marcelo was inducted into the EC-Council's CEH Hall of Fame in recognition of his outstanding career achievements.

Return to Index - Add to Google - ics Calendar file

WS - Thursday - 09:00-12:59 PDT

Title: Sold Out - Tracing The Pain Away - Practical Binary Tracing Techniques For Defeating Modern Malware Protections
When: Thursday, Aug 8, 09:00 - 12:59 PDT
Where: Springhill Suites/Sands - Map

Description:

Code obfuscation is fast becoming a normal part of modern Windows malware. Pioneered by Emotet and popularized by the Conti ransomware leaks, we now see even simple credential stealers using commercial grade code virtualization! The solution… if you can't reverse it, just run it! In this workshop we will cover different tracing techniques that can be used to bypass and extract information from protected code. The workshop is divided into modules covering tracing with x64dbg, dynamic binary instrumentation with PIN, and API tracing with DTrace. A challenge binary is provided with each module for students to practice and the final challenge is a real world malware sample that has been virtualized. This workshop is aimed at reverse engineers and malware analysts who have experience analyzing malware and are comfortable with debugging in userland. If you don't have experience with malware but you do have a few hours behind the debugger you should have no problem completing the workshop. Students must bring a laptop/workstation capable of running a Windows Virtual Machine (VM) and a preinstalled Windows 10 (64bit) 20H1(or later) VM with at least 50G of free space. You will be provided with detailed tools installation and setup instructions prior to the workshop

Speakers: Sean ,Serrgei Frankoff

SpeakerBio: Sean , Co-founder at OpenAnalysis

Sean, a co-founder of OpenAnalysis Inc., splits his time between reverse engineering, tracking malware and building automated malware analysis systems. Sean brings over a decade of experience working in a number of incident response, malware analysis and reverse engineering roles.

SpeakerBio: Serrgei Frankoff, Co-founder at OpenAnalysis

Sergei is a co-founder of OpenAnalysis Inc. When he is not reverse engineering malware Sergei is focused on building automation tools for malware analysis, and producing tutorials for the OALABS YouTube channel. With over a decade in the security industry Sergei has extensive experience working at the intersection of incident response and threat intelligence.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 09:00-12:59 PDT

Title: Sold Out - Traumatic Library Loading : If you want to use it, you have to implement it...
When: Friday, Aug 9, 09:00 - 12:59 PDT
Where: Springhill Suites/Dean Martin - Map

Description:

DLL Loading is one of the most important parts of the Windows system. When you install, run, use, or hack a system, you will always use DLL. This DLL mechanism has been exploited for several years for malware development through several techniques : DLL injection, DLL sideloading, Reflective DLL but do you really know how Windows is loading a DLL ? Do you know how it links all sections ? Which structures are used to store internally ? How does it resolve dependencies ? And are you able to design your own Perfect DLL Loader that fully integrate with the WIN32API? In this workshop, you will lose you sanity and dive into the Windows DLL mechanism. Armed with your decompiler and your brain, step by step, you will build your own (almost) Perfect DLL loader. You will try to load from the simple AMSI.DLL to the most complexe WINHTTP.DLL. At each step, you will dive deeper into the Windows DLL Loader and the Windows Internals. Malware developers, you will be able to use this code as a PE loader that never failed me for the last years and a DLL loader that does not raise the LoadImage kernel callback you can use on your own C2 beacon. WARNING: while this is a windows internal DISCOVERY discovery course, it is still a HIGHLY TECHNICAL workshop. You should have some entry-level knowledge on Windows systems, C programing and reverse engineering to fully enjoy the workshop. It is expected from the student to bring a laptop with either a Windows 10 or Windows 10 VM, a C compiler (Mingw or MSVC), a decompiler (IDA Free or Ghidra), the WinDBG debugger and the Sysinternals suite. I will personally use the following toolchain : WIN10, MSVC, IDA, WinDBG Preview.

SpeakerBio: Yoann Dequeker, Red Team Operator at Wavestone

Yoann Dequeker (@OtterHacker) is a red team operator at Wavestone entitle with OSCP and CRTO certification. Aside from his RedTeam engagements and his contributions to public projects such as Impacket, he spends time working on Malware Development to ease beacon deployment and EDR bypass during engagements and is currently developing a fully custom C2. His research leads him to present his results on several conferences such as LeHack (Paris), Insomni'hack (Swiss) or even through a 4-hour malware workshop at Defcon31 (Las Vegas). All along the year, he publishes several white papers on the techniques he discovered or upgraded and the vulnerabilities he found on public products.

Return to Index - Add to Google - ics Calendar file

WS - Friday - 09:00-12:59 PDT

Title: Sold Out - Whitebox Web Exploit Development
When: Friday, Aug 9, 09:00 - 12:59 PDT
Where: Springhill Suites/Dunes - Map

Description:

Gain experience popping root shells on real world web applications and taking your hacking skills to the next level. Students will learn accessible and powerful vulnerability discovery techniques to identify, exploit and chain vulnerabilities for root shells. Getting hands-on experience using free and widely available Linux utilities to debug and dynamically monitor applications, to more effectively discover and exploit vulnerabilities. Using a whitebox approach students will rapidly discover and exploit non-trivial bugs. A progressive hint system will be used during the labs to incrementally reveal step-by-step progressions of each exploit exercise in case students are stuck or fall behind. Course Objectives: --Students will gain hands-on experience analyzing and developing exploits for real world application vulnerabilities. --Students will learn how to discover vulnerabilities and subsequently weaponize them in an exploit chain to spawn remote shells on application servers. --Students will gain experience using open source linux tools like strace and tcpdump to analyze application behavior and isolate vulnerabilities. --Students will gain experience weaponizing web application vulnerabilities and writing exploits Upon Completion of this training, attendees will know: --How to identify situations where openbox application vulnerability assessments are appropriate and how to leverage this powerful context. --How to utilize openbox penetration testing methodologies to achieve more thorough and effective assessments. --How to leverage vulnerability chaining to assemble multiple medium criticality findings into a single remote root exploit.

Speakers: Cale Smith,Priyanka Joshi

SpeakerBio: Cale Smith, Amazon

Cale Smith is a nerd who loves both building but also breaking, so he can get better at building. He is passionate about understanding how anything and everything works, improving security along the way is just a bonus. Also, he is passionate about sharing his passion and created this course to pass along some of the more accessible techniques he has picked. His professional career originated exclusively as a builder, but has been focusing on the security and breaking side for the last 15 years. During that time he has dabbled in the web weenie life, cloud, binary, IoT and mobile most recently. Currently he manages a device oriented AppSec team at Amazon. While AFK he is probably riding a bike or climbing rocks.

SpeakerBio: Priyanka Joshi, Security Engineer, Ring AppSec at Amazon

Priyanka Joshi started her career through the academic path of computer engineering followed by a masters degree in information security. Her learning journey truly began doing security engineering in the industry. She discovered her passion in the identity space during her first software security engineer job at an ancient mid sized company. There she focused on research, development, maintenance and security testing of OAuth2.0/OpenID implementations for over two years. In her current appsec engineer role at Amazon, she enjoys working on secure design assessments, bug bounty triage and fix validation, consults and security testing of web services. Outside of work, she enjoys hiking, sketching, music, watching anime and reading manga.

Return to Index - Add to Google - ics Calendar file

IOTV - Friday - 14:00-15:59 PDT

Title: Solder your own cat shaped WiFi Haking tool
When: Friday, Aug 9, 14:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Test out your through-hole and surface mount soldering skills to create your own open-source, cat-themed hacking tool! The WiFi nugget is a microcontroller-powered WiFi hacking device you will then flash with a suite of WiFi tools to get started with offensive and defensive WiFi security techniques.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 12:00-12:20 PDT

Title: Solving the "Lover, Stalker, Killer" Murder with strings, grep, and Perl
When: Sunday, Aug 11, 12:00 - 12:20 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

Cari Farver did not disappear off the face of the Earth. She was murdered in cold blood, and her killer went on to impersonate her online, for over three years. The suspect hid their tracks with VPNs, proxies, and anonymizing apps. This talk will go behind the scenes of Netflix's "Lover, Stalker, Killer" to detail the open source software and bespoke methods used to prove a no-body homicide case based almost entirely on digital evidence.

Dateline NBC, S26E1 "Scorned" (2017) Rule, Leslie. "A Tangled Web: A Cyberstalker, a Deadly Obsession, and the Twisting Path to Justice". Citadel Press, 2020. Netflix, "Lover, Stalker, Killer" (2024)

SpeakerBio: Anthony Kava

Anthony Kava is a hacker and carries a badge. Got his start breaking Apple IIs then moved, somehow, to breaking baddies. Works as a cyber crime investigator and digital forensics examiner with a penchant for infosec. Kava is a recognized Soylent drinker, scourge to software vendors, and has been portrayed by a Canadian in a Lifetime movie. Dreams in Perl. Enjoys long walks on the dark web.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 18:05-19:05 PDT

Title: Something something Meshtastic Pip-Boy Personal Mesh with 150 km reach
When: Saturday, Aug 10, 18:05 - 19:05 PDT
Where: Virtual

Description:
SpeakerBio: Giglio

There once was a lad, brave and free Whose words I shall craft in glee "Meshtastic" he'd say With his Pip-Boy each day He traveled so far with amazing spree (limerick bio created by Private LLM)

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Space Grand Challenge Luna
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

The Space Grand Challenge (SGC) Program is a free virtual game-based cybersecurity/space competition CTF for middle and high school students built by Cal Poly students—Learn by Doing in action. The game is built on the UNITY gaming engine.

SpeakerBio: CalPoly
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Space Grand Challenge Luna
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

The Space Grand Challenge (SGC) Program is a free virtual game-based cybersecurity/space competition CTF for middle and high school students built by Cal Poly students—Learn by Doing in action. The game is built on the UNITY gaming engine.

SpeakerBio: CalPoly
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Space Grand Challenge Luna
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

The Space Grand Challenge (SGC) Program is a free virtual game-based cybersecurity/space competition CTF for middle and high school students built by Cal Poly students—Learn by Doing in action. The game is built on the UNITY gaming engine.

SpeakerBio: CalPoly
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 15:30-17:30 PDT

Title: Space Pirate Simulator
When: Friday, Aug 9, 15:30 - 17:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

It's time to go beyond hacking the planet! Join us for an offensive cybersecurity in space workshop. We will discuss the challenges that are introduced when attacking space vehicles and work with space industry software such as COSMOS, the ground station software used by NASA, and a modified version of NOS3, NASA's satellite simulator. Attendees will have access to cloud environments that contain an operator station, a ground station, and a simulated satellite. We will walk you through the basics of accessing, operating, and of course, attacking these stations for the ultimate goal of taking control of the satellite.

Speakers: Michael Butler,Jacob Oakley

SpeakerBio: Michael Butler

Michael Butler is a 14-year veteran of the offensive cybersecurity industry. He got his start conducting cyber warfare operations with the US Army and NSA. He has built two industry leading penetration testing teams. He is an expert in cloud security and has taught courses on hacking AWS, Azure, and GCP environments at BlackHat, at MITRE, and more. He has worked as a consultant, code reviewer, and penetration tester for ground station software.

SpeakerBio: Jacob Oakley
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: Space Systems Security CTF – Platform Security
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Launch into the thrilling world of cybersecurity, specifically designed for space systems! Learn the fundamentals to safeguard ground stations, communication links, and spacecrafts.

Engage in an immersive and fun CTF scenario. Apply your cybersecurity skills in real-time and see the direct impact of your decisions on our Space Systems Demonstrator. In this high-stakes scenario, you'll align with the Aurora Alliance in their critical mission to thwart Count Viktor Thunderclaw and the notorious Nebula Syndicate. The Syndicate threatens to destroy historic monuments around the world with their Space Laser unless their demands are met. Do you have what it takes to dismantle their malevolent plans?

Our beginner-level CTF kicks off as soon as the village opens—no pre-registration necessary. Just bring your laptop to access the CTF platform and your favorite packet decoding software (i.e. Wireshark). Expect the CTF to take you less than 1 hour to complete. Team collaboration is encouraged, and if you encounter obstacles, numerous hints are available to guide you. Excel in the challenge, and you could walk away with a CT Cubed SAO, an exclusive prize while supplies last.

SpeakerBio: CT Cubed

No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: Space Systems Security CTF – Platform Security
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Launch into the thrilling world of cybersecurity, specifically designed for space systems! Learn the fundamentals to safeguard ground stations, communication links, and spacecrafts.

Engage in an immersive and fun CTF scenario. Apply your cybersecurity skills in real-time and see the direct impact of your decisions on our Space Systems Demonstrator. In this high-stakes scenario, you'll align with the Aurora Alliance in their critical mission to thwart Count Viktor Thunderclaw and the notorious Nebula Syndicate. The Syndicate threatens to destroy historic monuments around the world with their Space Laser unless their demands are met. Do you have what it takes to dismantle their malevolent plans?

Our beginner-level CTF kicks off as soon as the village opens—no pre-registration necessary. Just bring your laptop to access the CTF platform and your favorite packet decoding software (i.e. Wireshark). Expect the CTF to take you less than 1 hour to complete. Team collaboration is encouraged, and if you encounter obstacles, numerous hints are available to guide you. Excel in the challenge, and you could walk away with a CT Cubed SAO, an exclusive prize while supplies last.

SpeakerBio: CT Cubed

No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: Space Systems Security CTF – Platform Security
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Launch into the thrilling world of cybersecurity, specifically designed for space systems! Learn the fundamentals to safeguard ground stations, communication links, and spacecrafts.

Engage in an immersive and fun CTF scenario. Apply your cybersecurity skills in real-time and see the direct impact of your decisions on our Space Systems Demonstrator. In this high-stakes scenario, you'll align with the Aurora Alliance in their critical mission to thwart Count Viktor Thunderclaw and the notorious Nebula Syndicate. The Syndicate threatens to destroy historic monuments around the world with their Space Laser unless their demands are met. Do you have what it takes to dismantle their malevolent plans?

Our beginner-level CTF kicks off as soon as the village opens—no pre-registration necessary. Just bring your laptop to access the CTF platform and your favorite packet decoding software (i.e. Wireshark). Expect the CTF to take you less than 1 hour to complete. Team collaboration is encouraged, and if you encounter obstacles, numerous hints are available to guide you. Excel in the challenge, and you could walk away with a CT Cubed SAO, an exclusive prize while supplies last.

SpeakerBio: CT Cubed

No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 10:00-12:59 PDT

Title: spacestudio and spacetower challenges
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Use spacestudio software to work through multiple challenges and scenarios. For instance:

Challenge 1: Analysis of the performance of the next GEN of satellites to size the ground segment.

Challenge 2: Assessment of propulsion system capabilities for initial orbit raising

Challenges for spacetower flight dynamic software will also be available.

Speakers: Exotrail,Hack-A-Sat

SpeakerBio: Exotrail
No BIO available
SpeakerBio: Hack-A-Sat
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Friday - 10:00-17:59 PDT

Title: spacestudio and spacetower challenges
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Use spacestudio software to work through multiple challenges and scenarios. For instance:

Challenge 1: Analysis of the performance of the next GEN of satellites to size the ground segment.

Challenge 2: Assessment of propulsion system capabilities for initial orbit raising

Challenges for spacetower flight dynamic software will also be available.

Speakers: Exotrail,Hack-A-Sat

SpeakerBio: Exotrail
No BIO available
SpeakerBio: Hack-A-Sat
No BIO available

Return to Index - Add to Google - ics Calendar file

ASV - Saturday - 10:00-17:59 PDT

Title: spacestudio and spacetower challenges
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02 - Map

Description:

Use spacestudio software to work through multiple challenges and scenarios. For instance:

Challenge 1: Analysis of the performance of the next GEN of satellites to size the ground segment.

Challenge 2: Assessment of propulsion system capabilities for initial orbit raising

Challenges for spacetower flight dynamic software will also be available.

Speakers: Exotrail,Hack-A-Sat

SpeakerBio: Exotrail
No BIO available
SpeakerBio: Hack-A-Sat
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 15:20-15:50 PDT

Title: Speed Bumps and Speed Hacks: Adventures in Car Manufacturers Security
When: Saturday, Aug 10, 15:20 - 15:50 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Since the first car hit the road, manufacturers have been obsessed with safety. But hey, as AI wisely points out, determining the absolute 'safest' car can be as subjective as trying to decide on the best pizza topping! So, we decided to shift gears… into the world of car manufacturers' (application) security.

In this talk, get ready for a wild ride as we unveil the security findings from our research, affecting at least eleven major car manufacturers. Buckle up, folks, because your favorite brand might be on our list—along with your personal info!

Bring popcorn to watch some proof-of-concept videos.

With this talk we aim to demonstrate:

- that modern Web Applications are still affected by old/traditional vulnerabilities,
- how security issues can be chained together to build real attacks/demonstrate impact,
- highlight a common pattern on running unpatched third-party software,
- how organizations benefit from a responsible disclosure policy.

Speakers:David Sopas,Paulo A. Silva

SpeakerBio: David Sopas

David Sopas leads a team of security researchers at Checkmarx and co-founder of Char49. With more than 15 years experience in pentesting and vulnerability research, he have been acknowledged by companies like Google, Yahoo!, eBay and Microsoft. Retired from this bug bounty hunting "career", Sopas now focus on IoT security and tries to learn new things every day.

SpeakerBio: Paulo A. Silva

With a bachelor's degree in Computer Sciences and 15+ years developing software, in the last 10 years, Paulo has been focused on security research, ethical hacking, and penetration testing. He is a long-term OWASP volunteer and project leader, being one of those responsible for the OWASP API Security Top 10. He has co-/authored several secure coding practices manuals such as the OWASP Go Secure Coding Practices and the Kotlin Secure Coding Practices guide.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 10:30-11:15 PDT

Title: Spies and Bytes: Victory in the Digital Age
When: Friday, Aug 9, 10:30 - 11:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

Join General Paul M. Nakasone, U.S. Army (Retired), for a deep dive into the realities of modern cyber warfare at DefCon. With critical stories from his extensive career, General Nakasone will expose the details of national security in the digital era.

The longest-serving leader of both the National Security Agency and U.S. Cyber Command, General Nakasone has been on the frontlines of America's cyber defense. He will share firsthand accounts of defending against nation-state hackers, securing critical infrastructure during global crises, and the strategies that kept adversaries at bay.

This talk will examine the evolving nature of conflict, where the battlefield extends into cyberspace and unique partnerships must be built to offer agility and resilience. General Nakasone will discuss the persistent threats posed by sophisticated hackers and the innovative defenses employed to counteract them. He'll delve into the importance of intelligence sharing, international alliances, and transparency in operations.

Looking ahead, General Nakasone will present a forward-thinking vision for the future of warfare. He'll highlight the necessity for adaptive cyber strategies, resilient defenses, and the cultivation of new leadership to address emerging threats.

SpeakerBio: General Paul M. Nakasone, Founding Director at Vanderbilt's Institute of National Security

Paul M. Nakasone, General, U.S. Army (Retired), is the founding director of Vanderbilt's Institute of National Security. With over three decades of distinguished service in the Army, his career began at the end of the Cold War and included pivotal moments such as being at the Pentagon on 9-11, deploying to combat zones in Iraq and Afghanistan, and spearheading cyber operations. His service spanned the Trump and Biden administrations, culminating as the Director of the National Security Agency and Commander of U.S. Cyber Command. Over nearly six years, he led the largest element of the US Intelligence Community and the Defense Department's cyber forces through three national elections, a global pandemic, and escalating threats to the homeland.

Throughout his career, General Nakasone has been a transformative leader, adept at navigating complex challenges. He implemented a persistent strategy in deploying cyber forces to combat nation-state hackers and expanded cooperation with international, interagency, and private sector partners to enhance insights into national adversaries. His efforts to increase operational transparency have significantly bolstered public trust in both the Agency and Command.

He remains deeply committed to fostering national service and leadership development.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 10:00-10:45 PDT

Title: Splitting the email atom: exploiting parsers to bypass access controls
When: Sunday, Aug 11, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

Websites often parse users' email addresses to identify their organisation. Unfortunately, parsing emails is far from straightforward thanks to a collection of ancient RFCs that everyone knows are crazy. You can probably see where this is going…

In this session, I'll introduce techniques for crafting RFC-compliant email addresses that bypass virtually all defences leading to broken assumptions, parser discrepancies and emails being routed to wildly unexpected destinations. I'll show you how to exploit multiple applications and libraries to spoof email domains, access internal systems protected by 'Zero Trust', and bypass employee-only registration barriers.

Then I'll introduce another class of attack - harmless-looking input transformed into malicious payloads by unwitting libraries, leading to yet more misrouted emails, and blind CSS injection on a well-known target.

I'll leave you with a full methodology and toolkit to identify and exploit your own targets, plus a CTF to develop your new skillset.

- Email parsing:
  - ♦ link
  - ♦ link
  - ♦ link
- CSS Exfiltration:
  - ♦ link
  - ♦ link
- Unicode:
  - ♦ link

SpeakerBio: Gareth Heyes, Researcher at PortSwigger

PortSwigger researcher Gareth Heyes is probably best known for smashing the AngularJS sandbox to pieces and creating super-elegant XSS vectors. He is the author of JavaScript for hackers. In his daily life at PortSwigger, Gareth can often be found creating new XSS vectors, and researching new techniques to attack web applications. He has a keen interest in hacking CSS to do wonderful, unexpected things and can often be seen experimenting with 3D pure CSS rooms, games and taking markup languages to the limit on his website. He's also the author of PortSwigger's XSS Cheat Sheet. In his spare time, he loves writing new BApp extensions such as Hackvertor.

Return to Index - Add to Google - ics Calendar file

AIxCC - Saturday - 11:30-11:50 PDT

Title: Spotting Deepfakes in a World with Generative AI
When: Saturday, Aug 10, 11:30 - 11:50 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Learn about DARPA's approach to developing tools to identify and flag multi-model media assets that have been generated or malicious purposes under the Semantic Forensics (SemaFor) program.

SpeakerBio: Dr. William Corvey, SEMAFOR Program Manager at DARPA Information Innovation Office

Dr. Wil Corvey joined DARPA as a program manager in the Information Innovation Office (I2O) in June 2020 to develop, execute, and transition programs in human language technology, artificial intelligence, and related areas. Prior to joining DARPA, Corvey served as a computational linguist with the United States Department of Defense. In this role they performed human language technology R&D, including multilingual natural language processing, information retrieval, and machine learning, with experience in knowledge-based, statistical, and neural techniques for automated linguistic analysis.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: spyVspy
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-G - Map

Description:

Embark on a thrilling espionage adventure with spyVspy! This contest imagines a world of spy games where contestants employ basic hacking, cryptography, and rogue skills to solve puzzles and uncover hidden caches strategically scattered throughout DEF CON (and beyond).

Contestants will engage in a real-world treasure hunt, where the locations of hidden caches are revealed by solving the types of puzzles you'd expect to see at DEF CON. Traditional ciphers, lockpicking, OSINT, and very basic hacking/pentesting skills may be required.

spyVspy is intended for players of all skill levels. Whether you're a seasoned double-agent or just learning to be a covert operative, you will be able to compete and have fun in this event. Whatever skills you think you're missing can probably be learned on-the-job anyway.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: spyVspy
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-02-02-G - Map

Description:

Embark on a thrilling espionage adventure with spyVspy! This contest imagines a world of spy games where contestants employ basic hacking, cryptography, and rogue skills to solve puzzles and uncover hidden caches strategically scattered throughout DEF CON (and beyond).

Contestants will engage in a real-world treasure hunt, where the locations of hidden caches are revealed by solving the types of puzzles you'd expect to see at DEF CON. Traditional ciphers, lockpicking, OSINT, and very basic hacking/pentesting skills may be required.

spyVspy is intended for players of all skill levels. Whether you're a seasoned double-agent or just learning to be a covert operative, you will be able to compete and have fun in this event. Whatever skills you think you're missing can probably be learned on-the-job anyway.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 14:00-14:45 PDT

Title: SQL Injection Isn't Dead: Smuggling Queries at the Protocol Level
When: Saturday, Aug 10, 14:00 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

SQL injections seem to be a solved problem; databases even have built-in support for prepared statements, leaving no room for injections. In this session, we will go a level deeper: instead of attacking the query syntax, we will explore smuggling attacks against database wire protocols, through which remote, unauthenticated attackers can inject entire (No)SQL statements into an application's database connection.

Using vulnerable database driver libraries as case studies, we will bring the concept of HTTP request smuggling to binary protocols. By corrupting the boundaries between protocol messages, we desynchronize an application and its database, allowing the insertion of malicious messages that lead to authentication bypasses, data leakage, and remote code execution.

To put our findings into context, we will explore the real-world applicability of this new concept by comparing how robust various languages and frameworks are against these attacks. We will also discuss how smuggling attacks are not specific to database wire protocols but affect all kinds of binary protocols, from databases over message queues to caching. We will end the session with inspirations for future research to explore the topic further.

- link
- link
- link
- link
- link
- link
- link

SpeakerBio: Paul Gerste, Vulnerability Researcher, R&D team at Sonar

Paul Gerste is a vulnerability researcher on Sonar's R&D team. He has a proven talent for finding security issues, demonstrated by his two successful Pwn2Own participations and discoveries in popular applications like Proton Mail, Visual Studio Code, and Rocket.Chat. When Paul is not at work, he enjoys playing CTFs with team FluxFingers and organizing Hack.lu CTF.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 12:00-12:30 PDT

Title: SQLi to Root Access: Exploiting a ISP infrastructure
When: Friday, Aug 9, 12:00 - 12:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

What if we play with the ISP? In this talk I am going to tell you how one day, something that started as a simple SQL injection, going through LFI, RCE, ended up in a pwn of an internet provider in my country that affected more than 25 cities, being able to intercept user traffic and other stuff.

SpeakerBio: Ignacio Daniel Navarro, Appication security / Ethical hacker

Ignacio Navarro, an Ethical Hacker and Security Researcher from Cordoba, Argentina. With around 6 years in the cybersecurity game, he's currently working as an Application Security. Their interests include code analysis, web application security, and cloud security.

Speaker at Hackers2Hackers, Security Fest, BSides, Diana Initiative, Hacktivity Budapest, 8.8, Ekoparty.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 13:00-13:45 PDT

Title: Sshamble: Unexpected Exposures in the Secure Shell
When: Friday, Aug 9, 13:00 - 13:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

The Secure Shell (SSH) has evolved from a remote shell service to a standardized secure transport that is second only to Transport Layer Security (TLS) in terms of exposure and popularity. SSH is no longer just for POSIX operating systems; SSH services can be found in everything from network devices, to source code forges, to Windows-based file transfer tools. While OpenSSH is still the most prominent implementation, it's now just one of dozens, and these include a handful of libraries that drive a wide range of applications. This presentation digs deep into SSH, the lesser-known implementations, many of the surprising security issues found along the way, and how to exploit them. As part of this talk, we will release an open source tool, dubbed "sshamble", that assists with research and security testing of SSH services.

Speakers:HD Moore,Rob King

SpeakerBio: HD Moore, CEO and Co-Founder at runZero

HD has focused on vulnerability research, network discovery, and software development since the 1990s. He is most recognized for creating Metasploit and is a passionate advocate for open-source software and vulnerability disclosure. HD serves as the CEO and co-founder of runZero, a provider of cutting-edge cyber asset attack surface management (CAASM) software and cloud services. Prior to founding runZero, he held leadership positions at Atredis Partners, Rapid7, and BreakingPoint. HD's professional journey began with exploring telephone networks, developing exploits for the Department of Defense, and breaking into financial institutions. When he's not working, he enjoys hacking on weird Go projects, building janky electronics, running in circles, and playing single-player RPGs.

SpeakerBio: Rob King, Director of Security Research at runZero

Rob King is the Director of Security Research at runZero. Over his career Rob has served as a senior researcher with KoreLogic, the architect for TippingPoint DVLabs, and helped get several startups off the ground. Rob helped design SC Magazine's Data Leakage Prevention Product of the Year for 2010, and was awarded the 3Com Innovator of the Year Award in 2009. He has been invited to speak at BlackHat, Shmoocon, SANS Network Security, and USENIX.

Return to Index - Add to Google - ics Calendar file

HRV - Friday - 11:30-12:30 PDT

Title: SSTV: How To Send Cat Memes Via Ham Radio
When: Friday, Aug 9, 11:30 - 12:30 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

SSTV - what the heck is slow scan TV and can you send cat memes with it? In this talk, hamster dives into the history, development and use of SSTV. From this, he will present the design for a wearable device to decode SSTV images and why he thought that was a good idea.

SpeakerBio: Hamster

Hamster is an engineer who watched too much MacGyver as a kid and is now doomed to invent more and more complicated ways to make the Angry Pixies dance.

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 13:15-13:59 PDT

Title: Stanford Digital Observatory
When: Saturday, Aug 10, 13:15 - 13:59 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

This talk with cover the networks that generate and spread misinformation over social media. This talk will dive deep into the challenges a think tank of this type is at risk of facing, and will give us an update on what is currently happening with the program. There will be a general overview of what happened and how the increasing threats came to be as well as an update on where things stand now.

SpeakerBio: Renée DiResta

My name is Renée DiResta. I'm the technical research manager at Stanford Internet Observatory, a cross-disciplinary program of research, teaching and policy engagement for the study of adversarial abuse in current information technologies. This means that I study the many ways that people attempt to manipulate, harass, or target others online. Sometimes that's influence operations, sometimes it's spam and scams, child safety issues, or novel ways of abusing generative AI technology. The internet is an ecosystem, and these things are interconnected: new technologies transform old problems. My name is Renée DiResta. I'm the technical research manager at Stanford Internet Observatory, a cross-disciplinary program of research, teaching and policy engagement for the study of adversarial abuse in current information technologies. This means that I study the many ways that people attempt to manipulate, harass, or target others online. Sometimes that's influence operations, sometimes it's spam and scams, child safety issues, or novel ways of abusing generative AI technology. The internet is an ecosystem, and these things are interconnected: new technologies transform old problems.I do research into novel and rapidly-developing problems, then communicate findings both to the public and to those best positioned to mitigate them. Over the years I've briefed world leaders and government bodies. I've advised Congress, the State Department, and myriad academic, civil society, and business organizations on the mechanics of online manipulation in its many forms, including computational propaganda, conspiracy theories, terrorist activity, and state-sponsored information warfare.

Return to Index - Add to Google - ics Calendar file

HRV - Saturday - 13:00-13:30 PDT

Title: Staying alive off the grid - using APRS and Lambdas to monitor temperature remotely
When: Saturday, Aug 10, 13:00 - 13:30 PDT
Where: LVCC West/Floor 3/W321 - Map

Description:

We love our furry friends, but they can't always join us - leaving a pet in a vehicle can be very risky, but may also be a necessity. Commercial solutions exist, however these all require monthly subscriptions and cell coverage in order to work. We are hackers! We can do better.

Using the Automatic Packet Reporting System (APRS), a digital communications standard that utilizes the 2 meter amateur radio band, I've built a monitoring platform that can alert on high or low temperatures even when cell service isn't available. By broadcasting a signal that can be picked up with commercial hand-held radios, backcountry monitoring is possible, and when inside coverage areas, an AWS Lambda, combined with the APRS.FI service enables real-time alerts through SMS messages.

In this talk, we'll go through the journey of building this off-the-grid temperature monitoring system, including evaluation of off-the-shelf tools commonly used for high-altitude ballooning, discussion of online APIs related to APRS and their limitations, and the risk modelling process related to a system designed for life safety. Attendees will be able to use this knowledge to build their own monitoring systems for use in vehicles, high-altitude balloons, or anywhere else remote monitoring is desired.

SpeakerBio: Kamikazi

No BIO available

Return to Index - Add to Google - ics Calendar file

BTV - Friday - 12:30-13:30 PDT

Title: Stealer Logs: Automation, Analysis, & Espionage in the World's Most Interesting Dataset
When: Friday, Aug 9, 12:30 - 13:30 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

This talk will cover:
- Timeline of stealer variants rise
- Common stealer behaviors
- The anatomy of a stealer log
- An overview of stealer log sales and trading points in cybercrime communities
- Insights from our analysis of millions of stealer logs
- Automation pipeline for stealer log collection
- Stealer log parsing and analysis
- Post-discovery response
- Other defensive strategies for stealer defense

What would someone know about you if they had all of the credentials saved on your computer? More importantly what would you know about the world if you had 60 million random samples of all of the credentials saved on the' computers of others? Join Eric Clay and Nick Ascoli as they dive into the fascinating world of stealer logs. Nick & Eric have spent more than 6 months examining the world's most comprehensive stealer log data set to understand.... well everything. Nick and Eric will not only go deep and examine one of the most interesting data sets for intelligence around, but will demonstrate data pipelines you can implement for collecting and operationalizing stealer logs for defense.

Speakers:

Eric Clay,Nick Ascoli

SpeakerBio: Eric Clay

Eric is a cybersecurity speaker and researcher with 8+ years in the field and 2+ years focused on cybercrime. Eric began his career as a GRC analyst before pivoting into network security data analysis and then Threat Intelligence. Eric now co-leads Flare's threat intelligence research team in addition to leading the marketing team.

SpeakerBio: Nick Ascoli

Nick Ascoli is an experienced threat researcher who is recognized for his expertise in data leaks, reconnaissance, and detection engineering. Nick is an active member of the cybersecurity community contributing to open-source projects, regularly appearing on podcasts (Cyberwire, Simply Cyber, etc.) and speaking at conferences (GrrCON, B-Sides, DEFCON Villages, SANS, etc.)

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 17:00-18:59 PDT

Title: Sticker Swap at DEF CON 32
When: Saturday, Aug 10, 17:00 - 18:59 PDT
Where: LVCC West/Floor 2/HallwayCon Lounge past W234 - Map

Description:

We've ran The UnOfficial DEF CON Sticker Swap for 5 years now. Maybe a few other things. This year will be the officially official DC Sticker Swap, come visit for sticker hacker culture and to swap a bit of history.

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 14:00-14:59 PDT

Title: Store bought is fine, sometimes!
When: Saturday, Aug 10, 14:00 - 14:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

Arguably one of the many unsexy topics in the space, but a super important consideration for those leading security programs and the ICs working on the individual components. This conversation will include an overview of the pros and cons of building vs buying decisions in a security program. Specific use cases, and maturity stages will be explored to help the audience understand how to work towards getting the balance right. Panelists with a wealth of diverse industry experience will talk through real world examples of what worked and what didn't, and lessons learned. We reserve the right to pull an Oprah Winfrey and leave jars of mayo under each seat to make this talk extra memorable.

Panelists' experience includes both IC and management, from startups to FAANG to giant enterprise.

Join us for this thrilling and dynamic panel as we extend the wisdom of The Barefoot Contessa, Ina Garten, to the security space. Why spend your precious time in the kitchen of your security program making absolutely everything from scratch, when store bought can be just fine sometimes? We'll discuss the pros and cons and considerations of build vs buy, in a talk that promises to capture the right balance of cynicism, nuance, and practicality. We know it's tempting to make our own mayo, but we've lived it and have to say - sometimes store bought is just fine. Prepare your well ack-shuallys, we're ready.

Speakers: Jason Craig,Lauren Proehl,Tina Velez,William Phillips

SpeakerBio: Jason Craig

Jason is a unicorn enthusiast and enjoys coffee, thrunting, and late apexes. Jason has worked for a few org's you've heard of, done some things, and prefers to be a quiet professional.

SpeakerBio: Lauren Proehl
No BIO available

SpeakerBio: Tina Velez, Growth Lead at ClearVector

Tina is the Growth Lead and resident muppet at ClearVector. Prior to that, Tina spent several years at Expel serving in a variety of roles including customer success, enterprise solutions architecture, solutions strategist, and management. Before making the transition full time to the amazing and harried world of security, she spent many years tech side in the SLED space, both within the state courts system and at a major public research university. She defines her happy place as one involving a lot of art, books, and snacks. Tina misses the days of dial up, and crappy MS Paint art. She is a founding member of ThruntCon.

SpeakerBio: William Phillips
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Friday - 17:30-17:50 PDT

Title: Stranger in a Changed Land
When: Friday, Aug 9, 17:30 - 17:50 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

What's it like to spend a career as a cyberdefender for the DoD and the nation, but homed inside of an intelligence agency? In this talk, I'll offer a historical and personal perspective based on 35 years at the National Security Agency as a vulnerability analyst for the defense, from junior analyst to executive manager. The common element across my career was the search for vulnerabilities in the name of defense - finding them, making sense of them, leading organizations to find them, and then translating that knowledge into action to prevent or manage them. I'll share lessons learned as cyberdefense evolved from a focus on mathematics and cryptography to systems and software; and from government security to a global internet. And we'll focus on the mission, technical, and cultural interplay of cyberdefense and offense/intelligence as it played out at NSA. War stories, culture clashes, bureaucratic mazes? Of course! But in the end, better security for all.

Communications Security, Computer Security, Information Security, Information Assurance, Defensive Information Operations, and several more - I'm very lucky to have ridden the World-Wide Wave we now call cybersecurity.

And I am very proud to have spent 35 years in Federal Service at the National Security Agency as part of the Information Assurance mission. The common element across my career was the search for vulnerabilities in the name of defense - finding vulnerabilities, making sense of them, leading organizations to find them, and then translating that knowledge into action to prevent or manage them.

That final challenge consumed the last third of my government career. How can we translate what we learn through product testing, Red Teams, Blue Teams, systems analysis, etc. into operational guidance, best practices, requirements, training, and security improvements? How can we bridge the gap between telling people what they are doing wrong, and helping them do what's right? This led to projects like the release of NSA Security Guides to the public (www.nsa.gov), involvement in open standards for security automation and information sharing, and an activity now known as the Critical Security Controls.

Since retirement in 2012, I have been able to continue to serve the cause of cyber defense through our work at the non-profit Center for Internet Security, and the Council on CyberSecurity before that. And I am very active in more volunteer cybersecurity causes than I can recall.

SpeakerBio: Tony Sager, Senior VP & Chief Evangelist at Center for Internet Security (CIS)

Tony is currently Senior VP & Chief Evangelist for the Center for Internet Security (CIS), leading a wide variety of strategic, partnership, and outreach activities. He led the work which later became known as the CIS Critical Security Controls – an independent, volunteer-developed, cyber defense best practices program which is used throughout the industry. Tony has led numerous other activities to develop, share, scale, and sustain effective defensive cyber practices for worldwide adoption.

In addition to his duties at CIS, Tony is a volunteer in numerous cyber community service activities: inaugural member of the DHS/CISA Cyber Safety Review Board; Advisor to the Minnesota Cyber Security Summit; Advisory Boards for several local schools and colleges; formerly a member of the National Academy of Sciences Cyber Resilience Forum; and service on numerous national-level study groups and advisory panels.

Tony retired from the National Security Agency in 2012 after 34 years as a mathematician, computer scientist, and executive manager. As one of the Agency’s first Software Vulnerability Analysts, he helped create and led two premier NSA cyber defense organizations (the System and Network Attack Center, and the Vulnerability Analysis and Operations Group). In 2001, he led the release of NSA security guidance to the public and expanded NSA’s role in the development of open standards for security.

In 2023, Tony was inducted into the Cybersecurity Hall of Fame.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 16:00-16:30 PDT

Title: Structural Insights: PDF Analysis for Detecting and Defending Against Threats
When: Friday, Aug 9, 16:00 - 16:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

We'll walk through the structures of a PDF, analyzing each part of it, demonstrating how Threat Actors work in the inclusion of malicious components in the structures of the file, in addition to demonstrating the collection of IOC(Indicators of Attack)s and how to build IOA(Indicators of Attack) for analysis by behavior, to anticipate new attacks. Demonstrating structures in the binaries as a PDF(header/ body/cross-reference table/trailer) and performing a comparison of malicious PDFs, explaining how each session works within a binary, what are the techniques used such as packers, obfuscation with JavaScript (PDF) and more, explaining too about some anti-disassembly techniques, demonstrating as a is the action of these malware's and where it would be possible to "include" a malicious code.

SpeakerBio: Filipi Pires, Founder at Black&White Technology

I've been working as Security and Threat Researcher and Cybersecurity Advocate at senhasegura, Founder at Black&White Technology, Cybersecurity Advocate, Snyk Ambassador, Application Security Specialist and Hacking is NOT a crime Advocate. International Speaker at Security and New technologies events in many countries such as US, Canada, France, Spain, Germany, Poland, and others, I've served as University Professor in Graduation and MBA courses at Brazilian colleges, in addition, I'm Creator and Instructor of the Course - Malware Attack Types with Kill Chain Methodology (PentestMagazine), PowerShell and Windows for Red Teamers(PentestMagazine) and Malware Analysis - Fundamentals (HackerSec).

Return to Index - Add to Google - ics Calendar file

XRV - Saturday - 11:30-11:59 PDT

Title: Student Engagement Doesn't Have to Suck
When: Saturday, Aug 10, 11:30 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Hacking Education for better outcomes / teaching in the metaverse

SpeakerBio: Dr. Muhsinah Morris, Founder at Metaverse United, LLC

Meet the first ever Metaversity Director, Dr. Muhsinah Lateefah Morris. A BS graduate of the HBCU CAU. She obtained an MS & PhD from the Harvard of the South, Emory University in Biomolecular Chemistry. Dr. Morris has been part of and leading Morehouse's Metaversity project since the Spring of 2021. She's won awards for Teaching Excellence, Best Emerging Technology and Innovation, and First Place Unconventional Innovation in Industry. She resides in McDonough GA with her husband and five sons. One of her sons has autism and she advocates for the entire autism community. She's a VR pioneer in education and is transforming learning globally. She is affectionately known as Dr. M.O.M. (Molder of Minds) by all her students. She continues to mold the minds of educators and students globally in the Metaverse. Her future is authentic transformation of the educational system for our future leaders using immersive technologies in the Metaverse. More recently, she founded Metaverse United, LLC where she helps people find where they belong in the embodiment of the internet called the Metaverse. Learn more at UnitetheMetaverse.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 11:30-12:15 PDT

Title: Sudos and Sudon’ts - Peering inside Sudo for Windows
When: Saturday, Aug 10, 11:30 - 12:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

In February 2024, Microsoft announced the release of Sudo for Windows for Windows 11 Insider Preview[1]. Like the Unix sudo utility, it provides a method for users to run commands with elevated permissions. This talk will share the results of an analysis of Sudo for Windows, starting with a summary of the information provided by Microsoft. From there, we will explore the architecture used to coordinate the elevation of the specified process, the ALPC service used to communicate between elevated and non-elevated processes, how Rust interoperates with Windows APIs, and the path resolution process for files and relative paths. As part of that journey, we will discuss a few discovered security issues.

This presentation will be valuable to anyone with an interest in Windows reverse engineering or Rust memory safety. A conceptual understanding of Windows Inter-Process Communication (IPC) and heap allocation may make parts of the talk more approachable, but the main ideas will be accessible to anyone with a high-level understanding of process memory layout (stack vs heap).

1. link
2. link
3. link
4. link
5. link
6. link
7. link

SpeakerBio: Michael "mtu" Torres, Senior Security Engineer, Network Infrastructure Security at Google

mtu, otherwise known as Michael Torres, is a Senior Security Engineer in the Network Infrastructure Security team at Google, where his primary focus is on Operational Technology systems. Michael is also a Staff Sergeant in the United States Marine Corps Reserve, where he has been responsible for planning and conducting both offensive and defensive cyber operations. He is passionate about sharing knowledge to benefit others, and is an active volunteer for VetSec (veteransec.org), a charity focused on helping military veterans have successful careers in cybersecurity.

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 11:00-11:50 PDT

Title: Supercharge your vuln finding workflow with automated labs: How Ludus made it rain creds from SCCM
When: Sunday, Aug 11, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

What if you could set up a full Active Directory network, with ADCS, SCCM, and Elastic EDR with one command, on hardware you control, with parameters you define? Come with us as we explore the power of automated labs NOT based on pre-configured static templates, instead built on-demand. This talk will explore the past, present, and future of automated cybersecurity test environments that enable you to get hands-on cybersecurity experience without spending a decade becoming a sysadmin first. It will also discuss how we used our lab to find a common misconfiguration in SCCM that was exposing Domain Admin credentials on the public internet! You'll walk away with a new SCCM tool and an open source tool to create your own labs, as well as the framework and ideas to build your own sharable modules.

Speakers: Erik Hunstad,Alberto Rodriguez

SpeakerBio: Erik Hunstad
No BIO available
SpeakerBio: Alberto Rodriguez
No BIO available

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 13:30-13:45 PDT

Title: Surprise Talk
When: Friday, Aug 9, 13:30 - 13:45 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-02 - Map

Description:

SpeakerBio: Rachel Cummings, Associate Professor of Industrial Engineering and Operations Research at Columbia University

Dr. Rachel Cummings is an Associate Professor of Industrial Engineering and Operations Research and (by courtesy) Computer Science at Columbia University, where she is also a member of the Data Science Institute and co-chairs the Cybersecurity Research Center. She is also a Fellow at the Center for Democracy & Technology. Before joining Columbia, she was an Assistant Professor of Industrial and Systems Engineering and (by courtesy) Computer Science at the Georgia Institute of Technology, and she previously received her Ph.D. in Computing and Mathematical Sciences at the California Institute of Technology. Her research interests lie primarily in data privacy, with connections to machine learning, algorithmic economics, optimization, statistics, and public policy. Dr. Cummings is the recipient of numerous awards including an NSF CAREER award, a DARPA Young Faculty Award, a DARPA Director's Fellowship, an Early Career Impact Award, multiple industry research awards, a Provost's Teaching Award, two doctoral dissertation awards, and Best Paper Awards at DISC 2014, CCS 2021, and SaTML 2023. Dr. Cummings also serves on the ACM U.S. Technology Policy Committee, the IEEE Standards Association, and the Future of Privacy Forum's Advisory Board.

Return to Index - Add to Google - ics Calendar file

Title: SWGRecon: Automate SWG Rules, Policy, and Bypass Enumeration
When: Friday, Aug 9, 12:40 - 13:25 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Enterprise users on their web browsers are prime targets for attackers, penetration testers, and red teamers. A common tactic involves tricking users into clicking on spear-phishing emails, downloading malicious documents or binaries, and subsequently compromising their systems. To mitigate these web-based initial access threats, enterprises deploy Secure Web Gateways (SWGs). SWGs are essentially SSL-intercepting cloud proxies that inspect web traffic, blocking attacks such as malicious file downloads, harmful websites, and scripts. Since all web traffic from users' browsers is routed through these proxies, SWGs have complete visibility into the scripts loading into users' browsers and the capability to block them.

In this talk, we will explore how to conduct reconnaissance against SWGs, identify the vendor and location, reconstruct the rules and policies applied, and identify bypasses based on these insights. We will introduce SWGRecon, a new tool designed to automate enumeration processes. This tool can be deployed as a JavaScript file for automatic enumeration and is complemented by a browser extension for certain scenarios. Our techniques have been rigorously tested against all the leading vendors in the market and have proven to be highly effective as of this writing.

Our primary objective is to raise awareness about how easily an attacker can deploy JavaScript via their website or inject it into a known website, uncovering loopholes in SWG rules and policies. By exploiting these loopholes, attackers can bypass protections and deliver malware or malicious websites directly to enterprise users' browsers.

SpeakerBio: Vivek Ramachandran, Founder at SquareX

Vivek Ramachandran is a security researcher, book author, speaker-trainer, and serial entrepreneur with over two decades of experience in offensive cybersecurity. He is currently the founder of SquareX, building a browser-native security product focused on detecting, mitigating, and threat-hunting web attacks against enterprise users and consumers. Prior to that, he was the founder of Pentester Academy (acquired in 2021), which has trained thousands of customers from government agencies, Fortune 500 companies, and enterprises from over 140+ countries. Before that, Vivek’s company built an 802.11ac monitoring product sold exclusively to defense agencies. Vivek discovered the Caffe Latte attack, broke WEP Cloaking, conceptualized enterprise Wi-Fi Backdoors, and created Chellam (Wi-Fi Firewall), WiMonitor Enterprise (802.11ac monitoring), Chigula (Wi-Fi traffic analysis via SQL), Deceptacon (IoT Honeypots), among others. He is the author of multiple five-star-rated books in offensive cybersecurity, which have sold thousands of copies worldwide and have been translated into multiple languages. He has been a speaker/trainer at top security conferences such as Blackhat USA, Europe and Abu Dhabi, DEFCON, Nullcon, Brucon, HITB, Hacktivity, and others. Vivek’s work in cybersecurity has been covered in Forbes, TechCrunch, and other popular media outlets. In a past life, he was one of the programmers of the 802.1x protocol and Port Security in Cisco’s 6500 Catalyst series of switches. He was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. He has also published multiple research papers in the field of DDoS, ARP Spoofing Detection, and Anomaly-based Intrusion Detection Systems. In 2021, he was awarded an honorary title of Regional Director of Cybersecurity by Microsoft for a period of three years, and in 2024 he joined the BlackHat Arsenal Review Board.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 10:00-10:59 PDT

Title: Taking off the blindfold: Detecting persistent threats on Draytek edge devices
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Advanced attackers are increasingly choosing edge devices as targets, many of which are security appliances such as VPNs and Firewalls. They run closed-source firmware, and defenders and researchers must understand it to assess its security and integrity. We faced this firsthand when a client that used Draytek equipment was compromised. With at least 500k Draytek routers exposed to the Internet globally, no working tools exist to extract their firmware and assist researchers and defenders working with them.

We reverse-engineered Draytek's firmware format, developed tools to extract it, and discovered that its RTOS kernel can load code modules dynamically. These stored modules remain active even after firmware upgrades, inadvertently facilitating persistent threats. We crafted and uploaded malicious modules using our tools and newly found vulnerabilities to achieve persistence.

End-users lack straightforward means to detect such compromises. In response to this threat, we developed our own module to assess the integrity of other modules loaded in memory, mitigating its impact. In our pursuit of a more secure internet, we are sharing our knowledge and opening our tools to the community, enabling observability, hardening, transparency, and vulnerability research on Draytek edge devices.

Speakers: Gastón Aznarez,Octavio Gianatiempo

SpeakerBio: Gastón Aznarez, Security Researcher at Faraday

Gastón Aznarez is a computer enthusiast who is passionate about cybersecurity. He earned a degree in Computer Science and began working in malware detection in firmware. He currently works as a Security Researcher at Faraday, specializing in discovering and exploiting vulnerabilities in IoT and embedded devices. Gastón also participates in CTF competitions and has shared his expertise as a speaker at different conferences.

SpeakerBio: Octavio Gianatiempo, Student, Computer Science at University of Buenos Aires

Octavio Gianatiempo is a Security Researcher at Faraday and a Computer Science student at the University of Buenos Aires. He's also a biologist with research experience in molecular biology and neuroscience. The necessity of analyzing complex biological data was his point of entry into programming. However, he wanted to gain a deeper understanding of how computers work, so he enrolled in Computer Science. As a Security Researcher at Faraday, he focuses on vulnerability research on IoT and embedded devices and fuzzing open and closed-source software to find new vulnerabilities and exploit them. He has presented his findings at various conferences, including DEFCON, Ekoparty, 8.8, and Nerdearla.

Octavio Gianatiempo trabaja como Security Researcher en Faraday y es estudiante de Ciencias de la Computación en la Universidad de Buenos Aires. También es biólogo con experiencia en biología molecular y neurociencia. Dentro de su rol en Faraday, se enfoca en sistemas embebidos e IoT, ingeniería inversa y fuzzing de código abierto y propietario para identificar vulnerabilidades y explotarlas. Ha presentado sus hallazgos en conferencias como DEF CON, Ekoparty, 8.8 y Nerdearla.

Return to Index - Add to Google - ics Calendar file

Title: Taming the Beast: Inside the Llama 3 Red Team Process
When: Friday, Aug 9, 15:30 - 16:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

In this presentation, the core AI Red Team at Meta will take you on a journey through the story of Red Teaming the Llama 3 Large Language Model. This talk is perfect for anyone eager to delve into the complexity of advanced model Red Teaming and safety, as well as how to perform their own research to find new attacks should attend this talk. We'll begin by exploring what AI Red Teaming is truly about, before exploring Meta's process and approaches on the topic. The team will detail our methodology for discovering new risks within complex AI capabilities, how emergent capabilities may breed emergent risks, what types of attacks we're looking to perform across different model capabilities and how or why the attacks even work. Moreover, we'll explore insights into which lessons from decades of security expertise can – and cannot – be applied as we venture into a new era of AI trust and safety.

The team will then move on to how we used automation to scale attacks up, our novel approach to multi-turn adversarial AI agents and the systems we built to benchmark safety across a set of different high-risk areas. We also plan to discuss advanced cyber-attacks (both human and automated), Meta's open benchmark CyberSecEvals and touch on Red Teaming for national security threats presented by state-of-the-art models. For each of these areas we'll touch on various assessment and measurement challenges, ending on where we see the AI Red Teaming industry gaps, as well as where AI Safety is heading at a rapid pace.

Speakers: Aaron "dyn" Grattafiori,Ivan Evtimov,Joanna Bitton,Maya Pavlova

SpeakerBio: Aaron "dyn" Grattafiori, Lead, AI Red Teaming at Meta

Aaron "dyn" Grattafiori is currently a lead for AI Red Teaming at Meta, leading the fight against the machines. Previously he spent over six years leading the "cyber" Red Team at Meta performing full-scale Operations against a wide array of objectives from insider threats and edge device compromises to simulated supply chain attacks, ransomware, custom rootkits and malware. Before working at Meta, Aaron was a Principal Consultant at NCC Group for many years working on application security assessments for leading software companies across web, mobile, cryptography, virtualization, containers as well as network security assessments. Aaron has spoken on a wide range of topics at security conferences such as BlackHat, DEF CON, Enigma, Toorcon, Source Seattle, Red Team Summit and more. When not hacking the LLM gibson, Aaron can be found on the slopes, the garage working on an old car or hiking the front range in Colorado.

SpeakerBio: Ivan Evtimov, Red Teaming Research Scientist, Gen AI Trust & Safety at Meta

Currently a red teaming research scientist at Meta Gen AI Trust & Safety. Ivan has been the tech lead for red teaming Llama 3, Code Llama, AudioBox, Seamless and participated as a red teamer in many other model and product releases. Ivan has also carried out AI research on cybersecurity safety, robustness to spurious correlations, and fairness in AI systems. Before Meta, Ivan was a member of the Computer Security and Privacy Lab and the Tech Policy Lab at the University of Washington, carrying out research on adversarial machine learning. He has also been spotted on a bike in the general vicinity of New York City.

SpeakerBio: Joanna Bitton, Software Engineer, GenAI Trust & Safety at Meta

Currently a software engineer on Meta's GenAI Trust & Safety, Joanna has been the lead for automation, safety and red teaming across many internal projects at Meta. An original member of the Facebook AI Red Team, she has worked on critical Responsible AI issues for over five years. She is also the author of AugLy, a data augmentation library for audio, image, text, and video to bypass classifiers and perform other attacks with over 5k GitHub stars. Joanna takes red teaming to heart, and can

neither confirm nor deny she was raised on a submarine.

SpeakerBio: Maya Pavlova, Software Engineer, GenAI Trust & Safety at Meta

Currently a software engineer on Meta's GenAI Trust & Safety, Maya Pavlova's main work these days has been on understanding how to bridge the gap between manual red teaming processes and automated solutions. Maya originally entered this world from the safety testing lens, previously working on scaling Responsible AI's fairness evaluation platforms, she has now pivoted to the interesting problem of how to automate AI red teaming attacks to build robust adversarial stress testing platforms.

Return to Index - Add to Google - ics Calendar file

TEV - Saturday - 10:00-17:59 PDT

Title: Tamper Evident Village Activities
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. Tamper-evident technologies are often confused with "tamper resistant" or "tamper proof" technologies which attempt to prevent tampering in the first place. Referred to individually as "seals," many tamper technologies are easy to destroy, but a destroyed (or missing) seal would provide evidence of tampering! The goal of the TEV is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

The Tamper-Evident Village includes the following contests and events:

- The Box; an electronic tamper challenge. An extremely realistic explosive with traps, alarms, and a timer ticking down. One mistake and BOOM, you're dead. Make every second count! Sign ups on-site when the TEV begins.
- Tamper-Evident King of the Hill; a full-featured tamper challenge. Tamper single items at your leisure and attempt to beat the current best. There can be only ONE! No sign ups required, play on-site when the TEV begins.
- Badge Counterfeiting Contest; submit your best forgery of a DEF CON human badge. Other target badges are also available for those looking for more counterfeit fun!
- For your viewing pleasure, collections of high-security tamper-evident seals from around the world.
- Presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.
- Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags.

Return to Index - Add to Google - ics Calendar file

TEV - Friday - 10:00-17:59 PDT

Title: Tamper Evident Village Activities
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. Tamper-evident technologies are often confused with "tamper resistant" or "tamper proof" technologies which attempt to prevent tampering in the first place. Referred to individually as "seals," many tamper technologies are easy to destroy, but a destroyed (or missing) seal would provide evidence of tampering! The goal of the TEV is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

The Tamper-Evident Village includes the following contests and events:

- The Box; an electronic tamper challenge. An extremely realistic explosive with traps, alarms, and a timer ticking down. One mistake and BOOM, you're dead. Make every second count! Sign ups on-site when the TEV begins.
- Tamper-Evident King of the Hill; a full-featured tamper challenge. Tamper single items at your leisure and attempt to beat the current best. There can be only ONE! No sign ups required, play on-site when the TEV begins.
- Badge Counterfeiting Contest; submit your best forgery of a DEF CON human badge. Other target badges are also available for those looking for more counterfeit fun!
- For your viewing pleasure, collections of high-security tamper-evident seals from around the world.
- Presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.
- Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags.

Return to Index - Add to Google - ics Calendar file

TEV - Sunday - 10:00-12:59 PDT

Title: Tamper Evident Village Activities
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-03 - Map

Description:

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. Tamper-evident technologies are often confused with "tamper resistant" or "tamper proof" technologies which attempt to prevent tampering in the first place. Referred to individually as "seals," many tamper technologies are easy to destroy, but a destroyed (or missing) seal would provide evidence of tampering! The goal of the TEV is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

The Tamper-Evident Village includes the following contests and events:

- The Box; an electronic tamper challenge. An extremely realistic explosive with traps, alarms, and a timer ticking down. One mistake and BOOM, you're dead. Make every second count! Sign ups on-site when the TEV begins.
- Tamper-Evident King of the Hill; a full-featured tamper challenge. Tamper single items at your leisure and attempt to beat the current best. There can be only ONE! No sign ups required, play on-site when the TEV begins.
- Badge Counterfeiting Contest; submit your best forgery of a DEF CON human badge. Other target badges are also available for those looking for more counterfeit fun!
- For your viewing pleasure, collections of high-security tamper-evident seals from around the world.
- Presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.
- Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags.

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 13:25-13:59 PDT

Title: Tapping the OSINT potential of Telegram
When: Friday, Aug 9, 13:25 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

This short talk explores the intelligence potential available in the Telegram messaging app, with particular focus on our novel work exploring its new “similar channels” feature. Telegram is a popular application with numerous, but labyrinthine, security settings and many ways to spill data. In November 2023, Telegram also launched a new “similar channels” recommender feature, explaining that upon joining a channel, users will be shown similar channels that were "selected automatically based on similarities in their subscriber bases.” We built a new tool, which we will release at DEFCON, to collect and analyze this similar channels data. We will then show how to use social network analysis techniques to uncover previously-hidden relationships between channels on the platform. In the course of collecting this OSINT for our own research projects, we uncovered evidence of numerous inauthentic channel networks that are being used to influence political discourse.

SpeakerBio: Megan Squire
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 17:00-17:20 PDT

Title: Techniques for Creating Process Injection Attacks with Advanced Return-Oriented Programming
When: Saturday, Aug 10, 17:00 - 17:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

This talk showcases techniques for process injection using advanced return-oriented programming (ROP). Process injection via ROP introduces significant hurdles, requiring many WinAPIs to be chained together, each with complex parameters and return values. We give practical details on how to best manage this. One seemingly insurmountable challenge is in identifying the target binary, as string comparison can be extremely difficult in ROP, as needed ROP gadgets may be lacking. We unveil a unique, universal solution, giving a reliable means of string comparison via ROP, which works all the time, allowing a specific process to be pinpointed and injected into via ROP.

We created numerous patterns for different WinAPIs, allowing for as many as a dozen ways of preparing a specific WinAPI via ROP, if using an approach centered around the PUSHAD instruction. With some WinAPIs, there are zero patterns for PUSHAD, forcing us to rely upon the much lauded “sniper” approach. We document all such variations of patterns for the WinAPIs in our demonstrated process injection. This research is not intended to demo a one-off example of process injection via ROP, but to provide a methodology that can be used time and time again, providing unique templates for others to use the same WinAPIs when attempting process injection via ROP.

1. Anonymous.(2019.) Cobalt Strike’s Process Injection: The Details. link
2. Hosseini, Ashkan. (2017). Ten Process Injection Techniques: A Technical Survey of Common and Trending Process Injection Techniques. link
3. Klein, A., & Kotler, I. (2019). Windows process injection in 2019. Black Hat USA, 2019.
4. Landau, Gabriel. (2021). What you need to know about Process Ghosting, a new executable image tampering attack. link
5. Mundbrod, N., Grambow, G., Kolb, J., & Reichert, M. (2015). Context-aware process injection: enhancing process flexibility by late extension of process instances. In On the Move to Meaningful Internet Systems: OTM 2015 Conferences: Confederated International Conferences: CoopIS, ODBASE, and C&TC 2015, Rhodes, Greece, October 26-30, 2015. Proceedings (pp. 127-145). Springer International Publishing.
6. Process Injection. MITRE ATT&CK. link
7. Process Injection. link
8. Unal, Ozan. (2020). Process Injection Techniques. link

Speakers: Bramwell Brizendine,Shiva Shashank Kusuma

SpeakerBio: Bramwell Brizendine, Assistant Professor at University of Alabama in Huntsville

Dr. Bramwell Brizendine completed his Ph.D. in Cyber Operations. A security researcher, currently Bramwell is an Assistant Professor at the University of Alabama in Huntsville, and he is the founding Director of the Vulnerability and Exploitation Research for Offensive and Novel Attacks (VERONA Lab). A cybersecurity expert, Bramwell has taught numerous undergraduate, graduate, and doctoral level courses in reverse engineering, software exploitation, advanced software exploitation, malware analysis, and offensive security. Additionally, Bramwell has authored several important cybersecurity tools, including JOP ROCKET, SHAREM, ShellWasp, and ROP ROCKET, which are open source and freely available. Bramwell was a PI on a $300,000 NSA research grant to develop a shellcode analysis framework, SHAREM. Bramwell has been a speaker at many top security conferences across the globe, including different regional variations of Black Hat, DEFCON, Hack in the Box, and more.

SpeakerBio: Shiva Shashank Kusuma, Computer Science Master's Student at University of Alabama in Huntsville

Shiva Shashank Kusuma, a Computer Science Master's student at the University of Alabama in Huntsville, has a deep interest in software engineering and cybersecurity. When not at work, Shiva enjoys reading about Blockchain, Web3, and AI.

Return to Index - Add to Google - ics Calendar file

TCV - Friday - 15:00-16:59 PDT

Title: Telecom Time Machine
When: Friday, Aug 9, 15:00 - 16:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

Join us at Telecom Village, DEFCON for a workshop on 2G and 3G network architectures and SS7 protocols. Gain a deep understanding of GSM and 3G networks, discover SS7 vulnerabilities, and engage in hands-on activities to simulate and analyze SS7 attacks. Designed for telecom professionals, cybersecurity enthusiasts, and researchers, this session aims to enhance your knowledge and security awareness in legacy telecom infrastructures

SpeakerBio: Nadeem Bagwan

With over 5 years of experience in telecom signaling security, Nadeem specialize in performing penetration testing for Radio Access Networks (RAN), SS7, Diameter, and GTP protocols, as well as telecom signaling forensics. He has extensive experience working in international environments, including the Middle East, South Asia, and Africa. His expertise spans various technologies, including SS7, Diameter, GTP, and 2G/3G/4G/5G core and radio access networks.

Return to Index - Add to Google - ics Calendar file

TCV - Sunday - 10:00-13:59 PDT

Title: Telecom Tinkerer CTF
When: Sunday, Aug 11, 10:00 - 13:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

Telecom Village is excited to announce "Telecom Tinkerer," Capture The Flag (CTF) event. Participants, known as Tinkerers, will simulate actions against various elements of a dummy target organization. Telecom Tinkerer will feature real-world simulation scenarios and challenges, allowing Tinkerers to simulate attacks and explore new attack vectors, tactics, techniques, and procedures (TTPs). The event will include combined exercises with different levels of threat/emulation and purple teaming, promoting a collaborative learning environment for both offensive and defensive strategies.

Return to Index - Add to Google - ics Calendar file

TCV - Friday - 10:00-10:59 PDT

Title: Telecom Village Inauguration
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W201 - Map

Description:

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 14:00-14:50 PDT

Title: Tempest c2: Use and Design
When: Saturday, Aug 10, 14:00 - 14:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Tempest is a new command and control framework written in Rust. The main goal of this framework is to prioritize ease of use for the hacker while also achieving elegant effectiveness on operations. Attendees will learn all about how to use the framework, with a focus on operational security and understanding the underlying code. This talk will go beyond just showing how to push buttons and learn steps for using a tool. We'll talk about how the c2 works, how post-ex modules work, how to avoid EDR detection, and how to make the most effective use of this or any c2 framework.

SpeakerBio: Kirk Trychel, Senior Red Team Engineer at Box.com

Kirk Trychel is a Senior Red Team Engineer with Box.com and a lifelong hacker. He has lead Red Teams with the Department of Defense, Secureworks Adversary Group, and CrowdStrike Adversary Emulations. Always eager to hack the newest technology, Kirk has produced original research across many areas of offensive security. His diverse experience combines with a passion to understand and expand attack surfaces, and do what defenders have not considered. Besides breaching systems, Kirk loves sharing his knowledge with the community and helping enhance organizations' security posture.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 10:00-11:45 PDT

Title: Tempest
When: Saturday, Aug 10, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W304 - Map

Description:

Tempest is a command and control framework written in 100% Rust. It began as a research project and personal challenge, but has grown into a very effective c2 framework. The original concept was to write a simple yet effective c2 framework, and design continues to focus on this simple goal. Because it started out as a research project with a learning goal, the framework is not directly based on any existing c2 frameworks and the vast majority of code will not be found anywhere else.

SpeakerBio: Kirk Trychel, Senior Red Team Engineer at Box.com

Kirk Trychel is a Senior Red Team Engineer with Box.com and a lifelong hacker. He has lead Red Teams with the Department of Defense, Secureworks Adversary Group, and CrowdStrike Adversary Emulations. Always eager to hack the newest technology, Kirk has produced original research across many areas of offensive security. His diverse experience combines with a passion to understand and expand attack surfaces, and do what defenders have not considered. Besides breaching systems, Kirk loves sharing his knowledge with the community and helping enhance organizations' security posture.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 12:00-13:45 PDT

Title: Tengu Marauder
When: Friday, Aug 9, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W305 - Map

Description:

The Tengu Marauder, derived from a previous security drone project, is a portable wheeled robot equipped with an ESP32 Marauder, currently in its testing phase. Designed for simplicity and efficiency, the Tengu Marauder serves as an alternative and interactive tool for WiFi network security testing. Its capabilities include WiFi scanning, deauthentication attacks, packet sniffing, and other wireless security tests. The compact design ensures ease of construction and maintenance using readily available parts and straightforward code integration. Essentially an advanced RC robot, the Tengu Marauder operates headless via XBee, providing a fun and engaging platform for testing the security of network-controlled devices over WiFi, such as IoT smart home devices and smaller WiFi-controlled drones like the Ryze Tello. This project would not have been possible without the development help, test runs, and support from the Philadelphia RAICES organization, the Philadelphia DEFCON group, and DeciSym.AI.

Speakers:Leonardo Serrano,Lexie Thach

SpeakerBio: Leonardo Serrano

Leonardo Serrano is a dedicated community organizer who spends his time learning more about the cyberz, connecting people, and supporting cool projects. His focus is primarily on threat modeling and the intersection of security architecture, process, and decision-making. Leo runs a hackerspace in Philadelphia called “The Tooolbox” with his partners where he hopes to showcase the amazing hackers who call Philadelphia home.

SpeakerBio: Lexie Thach

Lexie Thach has worked in cybersecurity for ten years in various positions. During this time, I developed a strong affinity for electrical engineering, programming, and robotics engineering. Despite not having a traditional academic background, I have extensive hands-on experience from my eight years in the US Air Force, specializing in cybersecurity and tactical networks for aircraft missions and operations. My focus on securing and testing the security of autonomous systems stems from these experiences, and I am passionate about sharing the techniques I have learned. Currently I run a local hackerspace in Philadelphia in support of DC215 called The Tooolbox where anyone can come to learn new hacking tools, try to build offensive or defensive security robots and we have 3D printers on standby for any prototyping people want.

Return to Index - Add to Google - ics Calendar file

CLV - Saturday - 10:30-11:10 PDT

Title: Terraform Unleashed: Crafting Custom Provider Exploits for Ultimate Control
When: Saturday, Aug 10, 10:30 - 11:10 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Terraform is a leading Infrastructure as Code (IaC) solution. It empowers developers to create custom providers for provisioning a wide array of infrastructure resources. Terraform provider functions as binary files on the server and interacts with terraform binary through RPC communication during terraform run. These providers, running as binary files on the Terraform server, enable developers to build custom functions that could be exploited to gain unauthorised access, potentially compromising the Terraform server, and exposing sensitive credentials and data.

In this talk, we'll explore the inner workings of custom provider modules and how their functions can be leveraged to exploit vulnerabilities in Terraform Enterprise. We will also cover developing a custom provider and utilities the same for gaining access to the terraform server extracting the cloud credentials. We will also present various architectural solutions around TFE and best practices for minimising these attack vectors. Furthermore, the session will provide actionable steps for assessing the security posture of custom providers to ensure a robust defence.

Speakers:Alex Foley,Rupali

SpeakerBio: Alex Foley

Alex Foley is a broadly experienced information technology and security professional with over 25 years of experience planning, managing, implementing, securing, supporting, and scaling diverse technology platforms and teams. He is currently the founder of Axl.net security and serves as Vciso to over 100 Plus startups focusing on cloud security posture management , architecture review and Compliance standards. Over the course of his career, he's had the opportunity to wear many hats and do "all the things" within product development and operations. This broad experience has enabled Alex to bring this depth of understanding to the CISO role for multiple organizations.

SpeakerBio: Rupali

Rupali brings over 8 years of cybersecurity experience, specializing in penetration testing and red teaming. Currently a Lead Security Architect at Axl.net security, she oversees cloud security and penetration testing engagements. Her credentials include notable certifications like OSCP, OSWE, AWS Security Specialist, and GCPN. She has presented at prominent conferences like Black Hat Asia, DevSecCon, and CoCon.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 10:00-11:45 PDT

Title: Testbed Virtual Factory
When: Saturday, Aug 10, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W306 - Map

Description:

As the landscape of industrial control systems (ICS) evolves, the security vulnerabilities inherent in these systems have become increasingly important. In response to this escalating situation, in this paper, we present the development of a virtualized cybersecurity research testbed tailored for these environments. Addressing the challenge of limited access to proprietary OT network data for research purposes, our this talk proposes a comprehensive framework for simulating industrial environments, aiming to facilitate the development and testing of cybersecurity solutions by providing functionalities for network traffic logging, attack impact simulation, generation of labeled multivariate time series sensor datasets, among others, bridging the gap between theoretical research and practical application needs, especially in situations of low data availability and data-driven cybersecurity research.

Speakers: Borja Pintos Castro,Camilo Piñón Blanco

SpeakerBio: Borja Pintos Castro, Researcher, Security and Privacy Area at Gradiant

Borja Pintos-Castro is passionate about cybersecurity, he spends the day reading and tinkering. He obtained a degree in Computer Engineering from the University of A Coruña. He also has a Master of Computer Security by the International University of La Rioja. Now, he is a researcher at Gradiant in the Security and Privacy Area and specifically in Cybersecurity industry 4.0 projects. Currently, he manages some industrial security projects, specifically analyzing network traffic and using honeypots to detect threats and attacks. He has the certification OSCP (PEN-200) from Offensive Security.

SpeakerBio: Camilo Piñón Blanco

Camilo Piñón-Blanco graduated in Telecommunication Technologies Engineering (2021) and Master in Telecommunication Engineering (2023) from the University of Vigo, both specializing in Telematics Engineering. He did his Bachelor's Thesis with GRADIANT, focused on detection of cyber-attacks in industrial networks with Machine Learning techniques. He has worked at the atlanTTic research center as a researcher, dealing with natural language processing and text data analysis. In 2022 he re-joined the GRADIANT as an Engineer-Researcher in Security and Privacy, within the Privacy & Security Analytics line, where he has done his Master's Thesis on anomaly detection in time series through UEBA and LSTM neural networks. His main lines of work are applied machine learning, data analysis and software development.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 11:00-11:50 PDT

Title: The Art of Critical Thinking through an Adversarial Mindset? (RTV Keynote)
When: Friday, Aug 9, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207 - Map

Description:

This keynote panel will highlight the significance of an adversarial mindset. Through this discussion, we will cover the advantages of approaching challenges from the perspective of an adversary in our professional journeys, and discuss practical ways in which we have implemented this mindset in our work.

Speakers: Ben "NahamSec" Sadeghipour,YTCracker,Barrett "pwneip" Darnell,Ryan M. "0dayCTF" Montgomery,Savannah "lazzslayer" Lazzara

SpeakerBio: Ben "NahamSec" Sadeghipour, Hacking Hub

Ben Sadeghipour, also known as NahamSec, is an ethical hacker, content creator, and keynote speaker. With a passion for cybersecurity that began in his teenage years, Ben's professional journey as a bug bounty hunter took off in 2014. He has played a role in helping organizations identify and remediate thousands of security vulnerabilities across a wide range of web and mobile applications in tech giants such as Amazon, Apple, Google, Airbnb, Snapchat, Zoom, and even the US Department of Defense. Ben helps others learn ethical hacking, bug bounty hunting, and reconnaissance techniques. He has also created training materials and content for conferences such as OWASP, DEFCON, and BSides.

SpeakerBio: YTCracker
No BIO available
SpeakerBio: Barrett "pwneip" Darnell
No BIO available
SpeakerBio: Ryan M. "0dayCTF" Montgomery
No BIO available
SpeakerBio: Savannah "lazzslayer" Lazzara
No BIO available

Return to Index - Add to Google - ics Calendar file

RCV - Saturday - 14:00-15:59 PDT

Title: The art of Pivoting in OSINT Investigations
When: Saturday, Aug 10, 14:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Join us for an immersive workshop designed for beginners and professionals looking to enhance their Open Source Intelligence (OSINT) skills. This workshop provides a technical guide to uncovering hidden connections and expanding investigative horizons using advanced OSINT techniques and tools. Participants will gain hands-on experience with leading OSINT tools, learn how to identify pivotal data points, and practice real-world pivoting strategies through interactive exercises and case studies.

This workshop is ideal for those seeking to refine their investigative methodologies and leverage cutting-edge OSINT practices for more effective and efficient investigations.

Topics: - OSINT Introduction and Walkthrough - Common tools and platforms - Data Sources - Understanding Pivoting - Identifying Pivot Points - Techniques and Tools - Data Correlation - Automation and Scripting - Case Study - Integrating OSINT with other Intel - Ethical and Legal Considerations

Skill Level: Beginner to Intermediate

SpeakerBio: Ram Ganesh
No BIO available

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 11:00-12:30 PDT

Title: The Bug Hunters Methodology Live - DEF CON Edition
When: Saturday, Aug 10, 11:00 - 12:30 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

The Bug Hunter's Methodology (TBHM) is a series of talks done by Jason exposing new advents in tools, tactics, and procedures used in web pentesting, bug bounty, and red teaming. In this talk, Jason will explore the mindset of approaching a hardened web target and how he breaks up finding vulnerabilities across its' stack. Many talks can teach you how to exploit a certain vulnerability, less can teach you how to find out where they are in complex pieces of software. TBHM also covers Jason's personal tips/tricks in the areas of automation, content discovery, javascript analysis, spidering, parameter analysis, functionality """"heatmapping"""", and more. The DEF CON edition will not be recorded and will release some free cutting edge content usually only available in Jasons live courses!

SpeakerBio: Jason Haddix, Arcanum Security

Jason Haddix, leads as CEO and “Hacker in Charge” of Arcanum Information Security, a premier firm specializing in assessments and training. Currently, he is the Field CISO for Flare.io and a Strategic Advisor to Bugcrowd. With a distinguished 20-year tenure in cybersecurity, Jason has previously held notable positions such as CISO at Ubisoft, Head of Trust at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has expertise across nearly all cybersecurity domains and is ranked 57th all-time on Bugcrowd’s bug bounty leaderboards.

Return to Index - Add to Google - ics Calendar file

AIxCC - Saturday - 14:00-14:20 PDT

Title: The Cat-and-Mouse Game of Adversarial Artificial Intelligence
When: Saturday, Aug 10, 14:00 - 14:20 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Adversarial AI has come a long way since its resurgence ten years ago. In this talk, we discuss how the landscape of attacks and defenses has shifted in recent years as a result of DARPA's program on Guaranteeing AI Robustness against Deception (GARD) as well as the rise of LLMs.

SpeakerBio: Alvaro Velasquez, GARD Program Manager at DARPA Information Innovation Office

Dr. Alvaro Velasquez joined DARPA in August of 2022 as a program manager focused on artificial intelligence. His current research interests are at the intersection of formal language theory and machine learning for sequential decision-making. He holds an interdisciplinary research record of more than 50 publications, including work in the areas of artificial intelligence, combinatorial optimization, and logic and circuit design.

Return to Index - Add to Google - ics Calendar file

AIxCC - Sunday - 13:15-13:59 PDT

Title: The Challenge in Building a Challenge
When: Sunday, Aug 11, 13:15 - 13:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

Technical challenge development team presentation

Return to Index - Add to Google - ics Calendar file

PHV - Friday - 12:00-12:59 PDT

Title: The Curious Case of Alice and Bob: What You Can (And Cannot!) Do as Digital Investigators
When: Friday, Aug 9, 12:00 - 12:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

The game is afoot! The curious case of Alice and Bob will explore beyond the surface of technical know-how. Attendees will navigate the intricate labyrinth of digital investigation, learning not just 'where' to seek digital clues – perhaps hidden in the registry – but crucially, 'why' these details matter and 'how' they fit into the larger puzzle of our investigation. Join me on a narrative adventure illuminating the practical use of tools in a real-world scenario. For both seasoned and aspiring digital sleuths, this talk aims to sharpen investigative skills, setting or recalibrating your expectations of what digital forensics can realistically achieve.

SpeakerBio: Catherine J. Ullman, Principle Technology Architect, Security at University at Buffalo

Dr. Catherine J. Ullman is a security researcher, speaker, author, and Principal Technology Architect, Security, at the University at Buffalo with over 20 years of highly technical experience. In her current role, Cathy is a digital forensics and incident response (DFIR) specialist, performing incident management, intrusion detection, investigative services, and personnel case resolution in a dynamic academic environment. She additionally builds security awareness among faculty and staff which educates and informs users about how to prevent and detect social engineering threats, and how to compute and digitally communicate safely. Cathy has presented at numerous information security conferences including DEF CON and Blue Team Con. Cathy is a contributor to the O'Reilly title 97 Things Every Information Professional Should Know and the author of the Wiley title The Active Defender. In her (minimal) spare time, she enjoys visiting her adopted two-toed sloth Flash at the Buffalo Zoo, researching death and the dead, and learning more about hacking things to make the world a more secure place.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 15:00-15:50 PDT

Title: The Curious Case of Stealer Logs: Access & Espionage in the World's Most Interesting Dataset
When: Saturday, Aug 10, 15:00 - 15:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

What would someone know about you if they had all of the credentials saved on your computer? More importantly what would you know about the world if you had 60 million random samples of all of the credentials saved on the' computers of others? Join Eric Clay and Nick Ascoli as they dive into the fascinating world of stealer logs. Nick & Eric have spent more than 6 months examining the world's most comprehensive stealer log data set to understand.... well everything. What can you learn from the credentials on a terrorists computer? What about a U.S. adversaries intelligence service or a ransomware group? And who actually killed JFK? Ok well maybe we haven't figured that one out yet. Nick and Eric will go deep and examine one of the most interesting data sets for intelligence since the advent of writing while maintaining a healthy sense of humor and more than a little fear of Polonium poisoning.

Speakers:Eric Clay,Nick Ascoli

SpeakerBio: Eric Clay

Eric is a cybersecurity speaker and researcher with 8+ years in the field and 2+ years focused on cybercrime. Eric began his career as a GRC analyst before pivoting into network security data analysis and then Threat Intelligence. Eric now co-leads Flare's threat intelligence research team in addition to leading the marketing team.

SpeakerBio: Nick Ascoli

Nick Ascoli is an experienced threat researcher who is recognized for his expertise in data leaks, reconnaissance, and detection engineering. Nick is an active member of the cybersecurity community contributing to open-source projects, regularly appearing on podcasts (Cyberwire, Simply Cyber, etc.) and speaking at conferences (GrrCON, B-Sides, DEFCON Villages, SANS, etc.)

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 17:20-17:50 PDT

Title: The Dark Side of Bug Bounty
When: Saturday, Aug 10, 17:20 - 17:50 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Bug bounty is an intricate game between the bug hunter, the clients, and the intermediary.

Like any game, it can be hacked. Like some games, it can be unfair.

Join Jason as he walks you through the darker secrets of bug bounty , tips and tricks to address them, and in some cases, commiserate that there are just bad realities to the game.

Jason will address the problems hardly talked about in the system, from a hacker, program owner, and platform runner.

SpeakerBio: Jason Haddix, Arcanum Security

Jason Haddix, leads as CEO and “Hacker in Charge” of Arcanum Information Security, a premier firm specializing in assessments and training. Currently, he is the Field CISO for Flare.io and a Strategic Advisor to Bugcrowd. With a distinguished 20-year tenure in cybersecurity, Jason has previously held notable positions such as CISO at Ubisoft, Head of Trust at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has expertise across nearly all cybersecurity domains and is ranked 57th all-time on Bugcrowd’s bug bounty leaderboards.

Return to Index - Add to Google - ics Calendar file

Title: The hack, the crash and two smoking barrels. (And all the times I (almost) killed an engineer.)
When: Sunday, Aug 11, 11:00 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

This is not a talk in which I will demonstrate exploit chains obtained from the underworld after signing with blood. It's about sharing meaningful stories from said underworld. The automotive underworld of huge corporations, short deadlines and lukewarm engineers. The one where companies fight for packing more and more functionality inside your computer on wheels, without paying attention to one of the things that our life actually depends on right now, cybersecurity.

While others talk about extremely significant remote vulnerabilities, I will focus on a high-level view of architecture and design of vehicles and where security fits in these processes. I will go through a journey of exploitation, from discovering 0days, to persuading engineers for the significance of a finding, by putting him in the driving seat and engaging the breaks mid-journey.

I will conclude, trying to understand why this is happening, why this behavior towards security still exists in the automotive industry, and how a small manufacturer managed to create one of the most secure embedded systems I faced in my career. All this, with a series of demos in real targets, and a real ECU on stage.

Our ultimate goal is to help people understand the state of the industry, spark the interest which can come out of hacking a computer on wheels, and try to raise awareness with a bit of hack, a bit of crash and two smoking barrels.

1. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... & Savage, S. (2010, May). Experimental security analysis of a modern automobile. In 2010 IEEE symposium on security and privacy (pp. 447-462). IEEE.
2. Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015(S 91), 1-91.
3. Cai, Z., Wang, A., Zhang, W., Gruffke, M., & Schweppe, H. (2019). 0-days & mitigations: roadways to exploit and secure connected BMW cars. Black Hat USA, 2019(39), 6.
4. Tencent. Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars.
5. link
6. UNECE, G. W. (2021). UN Regulation No. 155—Cyber Security and Cyber Security Management System. Technical Report. United Nations.
7. ISO. (2013). ISO 14229: Road vehicles — Unified Diagnostic Services (UDS).

SpeakerBio: Thomas "Cr0wTom" Sermpinis, Technical Director at Auxilium Pentest Labs

Thomas Sermpinis (a.k.a. Cr0wTom) is the Technical Director of Auxilium Pentest Labs and independent security researcher with main topics of interest in the automotive, industrial control, embedded device, and cryptography sectors. During his research, he published several academic papers, 0days and tools with the ultimate goal of making the world a safer place, but also helped almost 200 OEMs and Tier 1 automotive suppliers to achieve better security and develop more secure products.

Additionally, he spoke in several highly technical security conferences, presenting his research and trying to create safer streets for drivers, passengers, pedestrians, and everyone in the street, including Zer0Con, TyphoonCon, TROOPERS, DeepSec and others.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 10:00-10:50 PDT

Title: The Hybrid Horizon: Unleashing the Power of Azure Hybrid Integrations
When: Saturday, Aug 10, 10:00 - 10:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Ascension - Map

Description:

In the era of innovation and growth, technology and evolving landscape of cloud services, hybrid environments has become crucial for running smooth business operations. Integration between Cloud and On-Premise environments has helped organizations to build a bridge to fill the gap and increased flexibility, scalability, and agility in these digital world. This presentation delves into the complexities of various Azure offerings, investigating how malicious actors can exploit them to breach on-prem server.

We initiate our talk with a robust device management solution, demonstrating how attackers can enlist devices and manipulate certain functionalities to execute commands, which give complete access to Employee's Devices. Transitioning to another Azure feature, we dissect a connectivity option that enables PowerShell Remoting, effectively bridging the gap between Azure and on-premises servers.

Our exploration extends to Hybrid Workers which can be utilized to execute commands on on-premises servers, providing attackers with a stealthy pathway and can also be misused for persistence. We then examine Azure Arc and its Custom Script Extension, illustrating how it can be leveraged to execute commands within on-premises environments from the cloud.

The talk extends to the realm of Azure DevOps, where we shed light on abuse use case associated with custom agents being used for pipeline operations, granting unauthorized entry to on-prem resources. And finally, attention is drawn to the exploitation of web-based vulnerabilities, such as Remote Code Execution (RCE), to establish a foothold in on-prem networks which leverages Azure services for hosting on-prem applications.

Speakers: Chirag Savla,Raunak Parmar

SpeakerBio: Chirag Savla
No BIO available
SpeakerBio: Raunak Parmar
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 21:00-01:59 PDT

Title: The Illuminati Party
When: Saturday, Aug 10, 21:00 - 01:59 PDT
Where: LVCC West/Floor 3/W303-W304 - Map

Description:

The Illuminati Party is excited to open our doors once again to all those who wish to join us at DEF CON for an OPEN party welcoming all of our Hacker Family! Follow us on X (Twitter: @IlluminatiParty)

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 10:15-10:45 PDT

Title: The Immortal Retrofuturism of Mainframe Computers and How to Keep Them Safe
When: Sunday, Aug 11, 10:15 - 10:45 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

When you used your debit card today, do you know where that transaction was sent? Though it may conjure archival images of a 1950's IT room stocked with enormous, low-tech machines, Mainframe technology is both modernized and heavily relied upon today.

Mainframe architecture is some of the most reliable tech available, able to manage incredibly large input/output volumes with low risk of downtime and there are few signs of it being sunset in the decades to come. As protectors of the cyber landscape, understanding how mainframes are incorporated into a businesses topology and ways to secure mainframe architecture will remain important for any entity that utilizes this technology.

In this talk we'll explore the pervasiveness of mainframe technology, why it will remain relevant to the future landscape of mission critical-applications, and several trusted solutions for helping to secure these incredible computers.

SpeakerBio: Michelle Eggers

As a Security Consultant, Michelle Eggers executes penetration testing for a variety of client environments. After making a strong pivot from operations into proactive security, Michelle focuses on web application, mainframe, and network pentesting.

Michelle has contributed to the security community by speaking about mainframe and web application security at various cybersecurity conferences, volunteering with Black Girls Hack during Hacker Summer Camp, and driving forward interest in securing mission critical systems and critical infrastructure through authoring blog posts and social media content on the subjects.

Credentials and certifications earned include CompTIA Security+ and ISC2 Certified in Cybersecurity. She also holds a Bachelor of Science degree in Accounting, a Project Management Certificate from Cornell University, and an Evolve Security Certified Professional credential.

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 16:00-16:59 PDT

Title: The Implications of Cyberbiosecurity in Advanced Agricultural Systems
When: Friday, Aug 9, 16:00 - 16:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

The world is currently undergoing a rapid digital transformation sometimes referred to as the fourth industrial revolution. During this transformation, it is increasingly clear that many scientific fields are not prepared for this change. One specific area is agriculture. As the sector which creates global food supply, this critical infrastructure requires detailed assessment and research via newly developed technologies (Millett et al, 2019; Peccoud et al, 2018) . Despite its fundamental significance to modern civilization, many aspects of industrial agriculture have not yet adapted to the digital world. This is evident in the many vulnerabilities currently present within agricultural systems, as well as the lacking and fragmented nature of policy dictating cybersecurity stances– the field which intersects both cybersecurity and biosecurity to protect several areas within life sciences (Murch et al, 2018; Duncan et al, 2019; U.S. Department of Agriculture, 2022) . These looming oversights create dangers to advanced agricultural systems, which in turn poses risk to businesses, economies, and individuals. While there are various methods to reduce these risk factors, they ultimately depend on the careful consideration of cyberbiosecurity (CBS) by all involved. This includes the system developers, equipment engineers, and especially the end users - all of us. A conscientious team-effort can work to diminish risks and ultimately provide a safer environment for advanced agriculture and all who depend on it. This analysis explores numerous vulnerabilities within the system of advanced agriculture, discusses potential solutions to the escalating risks they present, and considers the achievable future of an advanced agricultural system which further implements the role of CBS.

SpeakerBio: Simone Stephen, Security Researcher

Simone is a lover of all things STEM but has a special place in her heart for Cyber. She graduated with my bachelor's in mechanical engineering in 2022, and attained a masters in Cybersecurity in December, 2023.

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 12:00-12:30 PDT

Title: The Interplay between Safety and Security in Aviation Systems
When: Sunday, Aug 11, 12:00 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Safety has been at the forefront of Civil Aviation since the formalization of DO-178, Software Considerations in Airborne Systems and Equipment Certification, in 1981. However, times have changed since then and we live in a world with seemingly limitless connectivity. DO-356A, Airworthiness Security Methods and Considerations, forms the cybersecurity bedrock in which aviation systems are designed and implemented. In this talk, participants will learn about how Safety and Security is applied to system design and how they interact with one another. Design Assurance Levels (DAL) and Security Assurance Levels (SAL) concepts are presented and explained what their purpose is. This talk is designed to appeal to the general cybersecurity community by introducing fundamentals of Safety analyses and discussing how Safety and Security interact with one another.

This talk will first touch upon fundamental documents that form the Certification basis for System Development (ARP4754B), System Safety (ARP4761A), and Security Considerations (DO-356A). From there, it walk through pieces that form a safety analysis and Design Assurance Level (DAL), walk through a system architecture under consideration, and learn about how Safety and requirements in a system can be used to inform the Threat Model for the system. From there, we end with a discussion on how Security Mitigations are assigned Security Assurance Level (SAL) and what this means for developers.

SpeakerBio: Lillian Ash Baker, Product Security Engineer at The Boeing Company/Wisk Aero

Lillian Ash Baker (aka Zap!) is a Sr. Product Security Engineer with The Boeing Company and Wisk Aero, securing the next generation of civil aviation aircraft. She is responsible for driving cybersecurity requirements across the entire aircraft ecosystem and maintaining DO-356/326 compliance. Prior to their time in Product Security, Lily was at Collins Aerospace for 15 years, responsible for the development, test, manufacturing, and integration of civil avionics equipment with a focus on Navigation and Inertial Systems. They have dealt with civil avionics certification to ARP-4754A, DO-160, DO-178, D…Ok, you get the idea. From particle accelerators to inertial flight testing, Lily has plenty Certified Scars and their stories to tell. When not designing aircraft, she volunteers as the CFP Organizer at the Aerospace Village.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 12:00-13:45 PDT

Title: The Metasploit Framework v6.4
When: Saturday, Aug 10, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W304 - Map

Description:

The Metasploit Framework released version 6.4 earlier this year, including multiple improvements to Kerberos-related attack workflows. The latest changes added support for forging diamond and sapphire tickets, as well as dumping tickets from compromised hosts. Metasploit users can now exploit unconstrained delegation in Active Directory environments for privilege escalation as well as use pass-the-ticket authentication for the Windows secrets dump module. These new Kerberos improvements increase the ways in which tickets can be forged, gathered, as well as used. Additionally, Metasploit has added support for new protocol based sessions, allowing users to interact with targets without uploading payloads, thus increasing their evasive capabilities. These new sessions can be established to database, SMB and LDAP servers. Once opened, they enable users to interact and run post modules with them, all without running a payload on the remote host. Finally, version 6.4 includes a complete overhaul of how Metasploit handles its own DNS queries. These improvements ensure that users pivoting their traffic over compromised hosts are not leaking their queries and offer a high degree of control over how queries should be resolved. This demonstration will cover these latest improvements and show how the changes can be combined for new, streamlined attack workflows using the latest Metasploit release.

Speakers: Jack Heysel,Spencer McIntyre

SpeakerBio: Jack Heysel, Senior Security Researcher at Rapid7

Jack Heysel is a Senior Security Researcher at Rapid7, where he contributes to and helps maintain the Metasploit Framework. Jack started at Rapid7 in 2016 working on their vulnerability management solution. He transitioned to the Metasploit team in 2021 and has been happily writing and reviewing exploits ever since. While AFK, Jack enjoys exploring the mountains and outdoors that surround his home.

SpeakerBio: Spencer McIntyre, Security Research Manager at Rapid7

Spencer McIntyre is a Security Research Manager at Rapid7, where he works on the Metasploit Framework. He has been contributing to Metasploit since 2010, a committer since 2014, and a core team member at Rapid7 since 2019. Previously, Spencer worked at a consulting firm working with clients from various industries, including healthcare, energy, and manufacturing. He is an avid open-source contributor and comic book reader.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 16:00-16:30 PDT

Title: The Missing Link - How we collect and leverage SBOMs
When: Saturday, Aug 10, 16:00 - 16:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

There is some debate as to how SBOMs can enhance vulnerability management practices, and some believe that collecting SBOMs from internal teams or suppliers is too difficult and time-consuming. Learn how Schneider Electric has collected thousands of our product SBOMs and how we are leveraging the SBOMs as part of our corporate product CERT to quickly analyze and focus our attention when time is of importance. This presentation describes how we modified our policies and processes to collect, generate, and store thousands of SBOMs. You will hear how we have leveraged SBOMs during the Log4j and OpenSSL vulnerability events. Then we will conclude with key learnings, suggestions, and opportunities for improvement.

SpeakerBio: Cassie Crossley, Vice President, Supply Chain Security, Cybersecurity & Product Security Office at Schneider Electric

Cassie Crossley, Vice President, Supply Chain Security in the global Cybersecurity & Product Security Office at Schneider Electric, is an experienced cybersecurity technology executive in Information Technology and Product Development and author of "Software Supply Chain Security: Securing the End-to-End Supply Chain for Software, Firmware, and Hardware." She has many years of business and technical leadership experience in supply chain security, cybersecurity, product/application security, software/firmware development, program management, and data privacy. Ms. Crossley has designed frameworks and operating models for end-to-end security in software development lifecycles, third party risk management, cybersecurity governance, and cybersecurity initiatives. She has an M.B.A. from California State University, Fresno, and her Bachelor of Science degree in Technical and Professional Communication with a specialization in Computer Science.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 10:00-10:45 PDT

Title: The not-so-silent type: Breaking network crypto in almost every popular Chinese keyboard app
When: Sunday, Aug 11, 10:00 - 10:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

People who don't type Chinese might be surprised to learn that popular Chinese Input Method Editor (IME) keyboards can act as keyloggers; they transmit your keystrokes over the Internet to enable "cloud-based" support features to improve character prediction when typing.

Everyone might be surprised to learn that these keyloggers, which were already collecting everything you type into your device, were doing it *insecurely*.

In this talk, we will describe how we systematically exploited every single popular Chinese IME keyboard vendor's home-rolled network encryption protocol. Namely, we show how any network eavesdropper can read the keystrokes of what users of these vendors' keyboards are typing. The affected keyboards include the three most popular Chinese IME keyboards, Sogou IME, Baidu IME, and iFlytek IME, collectively used by almost 800 million users, as well as default and pre-installed keyboards on basically every popular Android mobile device except for Huawei's. We also discuss how we got here, re-affirm the age-old adage, "Don't roll your own crypto!", and call on hackers around the world to help us move towards HTTPS everywhere in understudied app ecosystems.

link

link

Speakers: Jeffrey Knockel,Mona Wang

SpeakerBio: Jeffrey Knockel, Senior Research Associate at Citizen Lab

Jeffrey Knockel is a Senior Research Associate at the Citizen Lab. In his research, he seeks to bring transparency to censorship, surveillance, and other harmful software behavior.

SpeakerBio: Mona Wang, PhD candidate in Computer Science at Princeton University

Mona Wang is a PhD candidate in Computer Science at Princeton University specializing in network security and privacy. As an Open Technology Fellow at the Citizen Lab, she studied various proprietary encryption protocols used by popular Chinese mobile applications.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 15:00-17:30 PDT

Title: The Open Source Fortress: Finding Vulnerabilities in Your Codebase Using Open Source Tools
When: Friday, Aug 9, 15:00 - 17:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Classroom - Map

Description:

Regardless of where it is hosted, a codebase could end up in the hands of malicious actors. Aside from the open source scenario, attackers may utilize sophisticated techniques to access and download it. An example is Okta's 2022 breach, in which the source code of the identity and access management platform was obtained from GitHub.

Developers are advised to adopt a shift-left approach, uncovering as many code flaws as possible before releasing it to the public.

"The Open Source Fortress" will provide a framework for detecting vulnerabilities in codebases with open-source tools. The examples imply the discovery of vulnerabilities in a custom, purposefully vulnerable codebase written in C and Python. Static techniques such as symbolic execution, secret scanning, code querying, and dependency scanning will be discussed, as will dynamic techniques such as fuzzing.

SpeakerBio: iosifache

Andrei spent 2022 as a technical leader for a start-up that specialises in automating cybersecurity solutions, as well as being a security engineer in the Romanian Army. After determining that the start-up idea was unviable, he left the public sector and accepted a position at Canonical, working to secure Ubuntu and its open-source components.

Subsequently, he relocated to Switzerland and joined Snap Inc., where he helps make Snapchat a safer platform for our users, free from spam and abuse.

Andrei's current focus is on software security. He has recently contributed to the open-source space and provided advice to start-ups on cybersecurity matters.

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 11:30-12:10 PDT

Title: The Oracle Awakens: Demystifying Privilege Escalation in the cloud
When: Friday, Aug 9, 11:30 - 12:10 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

In this talk, we explore privilege escalation mechanisms and paths within Oracle Cloud. Privilege escalation, the process by which an attacker gains elevated access and permissions beyond those intended by the cloud administrator, poses a significant threat in cloud environments and can significantly aid an attacker or pentester.

Our discussion will focus on identifying privilege escalation paths, understanding how cloud administrators can misconfigure policies, and the methods attackers can use to exploit these vulnerabilities. Through carefully designed scenarios and real-world examples, attendees will learn to recognize signs of privilege escalation, thereby enhancing their security posture.

Speakers:
Felipe Pr0teus,Lucas Cioffi

SpeakerBio:
Felipe Pr0teus

Felipe Espósito also known as Pr0teus, graduated in Information Technology at UNICAMP and has a master's degree in Systems and Computing Engineering from COPPE-UFRJ, both among the top technology universities in Brazil. He has over ten years of experience in information security and IT, with an emphasis on security monitoring, networking, data visualization, threat hunting, and Cloud Security. Over the last years he has worked as a Security Researcher for Tenchi Security, a Startup focused in third-party risk management, he also presented at respected conferences such as Hackers 2 Hackers Conference, BHACK, BSides (Las Vegas and São Paulo), FISL, Latinoware, SecTor, SANS SIEM Summit, and Defcon's CloudSec and Recon Village.

SpeakerBio:
Lucas Cioffi

Lucas Cioffi has been working with cybersecurity for 7 years, and focused in Cloud for the last 3. He has a blog where he shares tips and tricks for Cloud Security, and has published some open-source tools. He was a Cloud Security lecturer for a brazilian college in 2022, and is currently pursuing a Masters degree at USP.

Return to Index - Add to Google - ics Calendar file

Title: The Past, Present, and Future of Bioweapons
When: Saturday, Aug 10, 14:30 - 15:15 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Biological warfare is a phenomenon that spans human history, tracing its roots to ancient times rather than being a recent invention. To gain insights into bioweapons' current and future landscape, it is imperative to delve into historical examples of conventional biological warfare and understand how methods were devised and implemented.

However, amidst the exploration of historical precedents, it becomes evident that our optimism for the future hinges significantly on our ability to foster transparency and creativity within the global community. This optimism is intertwined with our comprehension of technological advancements, the rapid pace of innovation, the interconnectedness of various domains, and the imperative task of constructing practical defenses against emerging threats. It is crucial to acknowledge that despite the sophistication of technology, its efficacy remains intricately linked to human ingenuity. As a poignant reminder, our vulnerability lies in technological shortcomings and our collective failure of imagination. Creativity, a distinctly human attribute, stands as the cornerstone in the perpetual endeavor to safeguard against unforeseen adversities.

Furthermore, the discourse extends to establishing social norms and mores that are pivotal in shaping attitudes toward biological warfare. Addressing the proliferation of disinformation and its potential to fuel the proliferation and utilization of bioweapons becomes imperative. This discussion encompasses an exploration of prospective research endeavors and emerging initiatives leveraging artificial intelligence (AI) in the realm of bioweaponry. Notably, the utility of Generative AI in affecting societal shifts toward the normalization of bioweapon deployment warrants scrutiny. Additionally, the current societal landscape, particularly the desensitization of internet denizens to overt hostile actions, poses profound implications for the future trajectory of biological warfare.

In essence, a comprehensive understanding of historical precedents, coupled with a proactive approach towards fostering transparency, creativity, and the cultivation of robust societal norms, is indispensable in navigating the complexities of bioweapon proliferation. As we confront the intricate interplay between technological advancements and human agency, it is imperative to remain vigilant and resolute in our pursuit of a future safeguarded against the malevolent exploitation of biological agents.

Speakers: Lucas Potter,Meow-Ludo Disco Gamma Meow-Meow ,Xavier Palmer

SpeakerBio: Lucas Potter, Engineer at BiosView

Lucas has been an engineer with BiosView, specifically focusing on BioCyberSecurity, for the past five years. Previous efforts have resulted in 14 academic journal articles and 22 conference articles.

SpeakerBio: Meow-Ludo Disco Gamma Meow-Meow

Meow-Ludo is an Australian biohacker, serial political candidate, and general provocateur. He is interested in transdisciplinary technological systems and how they can be used and abused. He is perhaps most well known for taking the government to court over his right to use an implanted travel-pass, and through doing so opened up a conversation around the rights that individuals have over the technology they use that extended around the world. He is currently working on life extension gene therapy design and assisting with psilocybin therapies for depression.

SpeakerBio: Xavier Palmer

Xavier comes from multiple disciplines and is also part of the virtual lab, BiosView. He is fond of promoting positive and

creative projects with non-traditional students that foster curiosity and conversation around technologies that interface with all aspects of biology.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 15:00-15:25 PDT

Title: The People's Republic of Fieldbus: What to know about EPA
When: Friday, Aug 9, 15:00 - 15:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

Ethernet for Plant Automation (EPA) is one of the global variety of IEC 61158 standards, developed as a regionalized versions of Fieldbus standards, used predominantly in industrial settings with prohibitive latency and durability requirements. EPA in particular seems to be used exclusively in the People's Republic of China, and largely for power stations.

In this talk, I will cover the standard through both IEC and GB/T documents, both in English and Mandarin, the protocol's history used in sensitive national projects, and what supporting the standard is like. I'll even dive in to some example software and hardware that use the standard, and show some POC code for interacting with EPA devices, should you be lucky enough to find yourself on a network with an EPA-supported router or PLC.

SpeakerBio: Jonathan Reiter
No BIO available

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 13:30-13:55 PDT

Title: The perma-lag: why industrial cybersecurity will never be state-of-the-art
When: Saturday, Aug 10, 13:30 - 13:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

We've been talking about the gap in ICS cybersecurity features and functions for over a decade, but it seems like we're always confronting the same set of challenges. Despite all the progress in products, systems, regulations and oversight it feels like we're caught in an endless loop of vulnerabilities. The problem isn't in a lack of effort on anyone's behalf: it's in the fundamental market forces that drive the critical infrastructure investments we depend on. This presentation looks at these forces and shows how to work with them rather than agains them, no matter what your mission might be.

SpeakerBio: Kyle McMillan
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 10:00-10:45 PDT

Title: The Pwnie Awards
When: Saturday, Aug 10, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

The Pwnies are an annual awards ceremony celebrating and making fun of the achievements and failures of security researchers and the wider security community. Every year, members of the infosec community nominate the best research and exploits they've seen. The Pwnie Award nominations are judged by a panel of respected security researchers and former pwnie award recipients – the closest to a jury of peers a hacker is likely to ever get. At this event DEF CON attendees will get a first person look at some of the most groundbreaking research and hacks in the cyber security community of the past year, and the winners get some well deserved recognition from the broader community for the great work they've done.

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 16:30-17:29 PDT

Title: The Quantum Ethics and Skills Debates
When: Saturday, Aug 10, 16:30 - 17:29 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Join us for another round of our Oxford Union-style debates @ DEF CON! Chaired by Bob Gourley, we're extremely excited to bring you two debates this year - one on Quantum Ethics, and another on the Quantum Skills gap, feat. some of our most excellent speakers including Bruna Shinohara de Mendonça, Joan Arrow of the Quantum Ethics Project, and more!

Speakers: Bob Gourley,Bruna Shinohara de Mendonça,Joan Arrow

SpeakerBio: Bob Gourley
No BIO available
SpeakerBio: Bruna Shinohara de Mendonça

Bruna Shinohara is a Staff Scientist specialized in Quantum Technologies from Brazil, currently working at CMC Microsystems, Canada. She holds a PhD in Physics, focusing on Condensed Matter Theory and Quantum Computation. She is also engaged in science outreach and advocates for democratizing access to information.

SpeakerBio: Joan Arrow
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 11:00-11:45 PDT

Title: The Rise and Fall of Binary Exploitation
When: Saturday, Aug 10, 11:00 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

For the past 20+ years binary exploitation has been seen as the ultimate challenge and prize, when exploiting large applications and operating systems. During this period, the question of "How much longer will we be able to do this?" has been asked countless times, and with good reason. Memory safety and corruption issues with low-level languages have been an enormous challenge for OS and application developers. There are certainly efforts to move to "safer" languages such as Rust, but those languages need to mature a bit longer before they're able to stand up to the capabilities of a language like C++.

Thanks to exploit mitigations and memory protections, a large number of these vulnerabilities are not exploitable. There are the mature mitigations, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR), and then newer ones such as Control-flow Enforcement Technology (CET) and Virtualization Based Security (VBS). A large number of these mitigations are not enabled by default on the Windows OS, due to the fact that many need to be tested to ensure they do not break production applications. In this presentation, we will take a technical dive into the state of binary exploitation and the effectiveness of the many available mitigations, by looking at the way they're enforced.

SpeakerBio: Stephen Sims, Fellow Instructor at SANS Institute

Stephen Sims is an experienced vulnerability researcher and exploit developer, having discovered and privately disclosed many vulnerabilities affecting well-known browsers and OS kernels. He is co-author of the popular Gray Hat Hacking book series through McGraw-Hill, now in its 6th edition. He is a Fellow Instructor with the SANS Institute and author of some of their most advanced content covering exploit development and other offensive operations and security related topics. Stephen also runs the Off By One Security channel on YouTube, where he teaches offensive-related material, bringing on a wide variety of experts on to provide free training to the community.

Return to Index - Add to Google - ics Calendar file

CLV - Sunday - 11:45-12:20 PDT

Title: The Rise of the Planet of the Agents: LLM-based AI Agents and Cloud Security APIs
When: Sunday, Aug 11, 11:45 - 12:20 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

In the rapidly evolving domain of cloud security, the ability to dynamically interact with cloud services is crucial for security teams. Understanding cloud APIs is key to effectively managing everything from administrative tasks to security operations. Security researchers often face the challenge of selecting from numerous API definitions. What if there was a system capable of autonomously selecting the right APIs and intelligently chaining them to achieve specific goals?

In this presentation, I will share insights from my research on LLM-based AI agents. These agents utilize LLMs as reasoning engines, enabling them to handle complex tasks in natural language and autonomously determine their next actions based on user input and previous interactions. I will explain how we can transform Microsoft Graph API definitions into schemas that align with LLM function-calling capabilities. This transformation allows an LLM to select the appropriate tools and supply the correct arguments for an AI agent to execute. By integrating generative AI with cybersecurity, we can automate tasks and discover new ways to chain APIs for various operations, significantly enhancing the capabilities of security researchers to innovate in security operations and automation.

SpeakerBio: Roberto Rodriguez

Roberto Rodriguez, also known as Cyb3rWard0g in the Infosec community, is a respected security researcher at the Microsoft Security Research organization. He is well-known for his contributions to the field, including the creation of influential open-source projects such as the Threat Hunter Playbook, Security Datasets, OSSEM, SimuLand and ATT&CK Python Client. Roberto's work has had a significant impact on the cyber security community, promoting proactive threat hunting and knowledge sharing. His expertise and dedication have made a lasting impact on the industry and has helped shape the future of cyber security.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 14:00-14:30 PDT

Title: The Risk and Reward of Distributed Industrial Control
When: Friday, Aug 9, 14:00 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Economic efficiency and increasing automation mean that many industrial assets are remotely monitored and controlled. While some assets, such as oil production platforms, remain manned in isolated conditions, the ecosystem of renewable energy and distributed energy resources (DERs), pipelines, and other assets are increasingly unmanned with control extending over common information links. While this has been a boon for cost, it has also resulted in a radical extension of attack surface for cyber operations.

In this discussion, we will explore the nature of distributed industrial asset operation and the opportunities this presents for adversaries to infiltrate and potentially disrupt critical infrastructure operations. To make this point, we will review examples of adversary activity, from the 2022 ViaSat incident through historical pipeline intrusions (NOT Colonial!), showing how adversaries intentionally or inadvertently prey on brittle communication links for industrial disruption. We will conclude with a discussion of how these risks can be mitigated in a way that is sensible and economical, because wind farm operators won't lay their own dedicated fiber anytime soon.

SpeakerBio: Joe Slowik

Joe Slowik has over 15 years of experience across multiple cyber domains and problem sets. Currently Joe leads CTI functions for the MITRE ATT&CK project while also conducting critical infrastructure threat research and analysis. Previously Joe has worked in multiple roles spanning CTI, detection engineering, and threat hunting at organizations such as Dragos, Huntress, DomainTools, and Gigamon. Joe started his infosec journey with the US Navy and at Los Alamos National Laboratory.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 13:05-14:05 PDT

Title: The Sand Castle - The State of the MacOS Sandbox
When: Saturday, Aug 10, 13:05 - 14:05 PDT
Where: Virtual

Description:
SpeakerBio: Jonathan "JBO" Bar Or, Principal Security Researcher at Microsoft

Jonathan Bar Or ("JBO") is a Principal Security Researcher at Microsoft, working as the Microsoft Defender research architect for cross-platform. Jonathan has rich experience in vulnerability research, exploitation, cryptoanalysis, and offensive security in general.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 12:30-13:15 PDT

Title: The Secret Life of a Rogue Device - Lost IT Assets on the Public Marketplace
When: Saturday, Aug 10, 12:30 - 13:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

An ex-employee's work laptop, a secret hardware prototype, the company backup server, and classified government computers. What do these things have in common? They should never end up on the public market. Ask any IT department and they'll tell you that "it happens", but how serious is the problem and what's really at stake? This talk explores the interesting journey of a research project to learn the surprising answers to these questions.

Along the way we'll scrape over 150 million images from online listings in Western and Eastern second hand markets, hack together an OCR cluster out of old iPhones, reverse engineer well-obfuscated Chinese apps, and converse with secretive underground groups of collectors.

SpeakerBio: Matthew "mandatory" Bryant, Red Team Lead at Snapchat

mandatory (Mathew Bryant) is a passionate hacker currently leading the red team effort at Snapchat. In his personal time he’s published a variety of tools such as XSS Hunter, CursedChrome, and tarnish. His security research has been recognized in publications such as Forbes, The Washington Post, CBS News, Techcrunch, and The Huffington Post. He has previously presented at DEF CON, Blackhat, RSA, Kiwicon, Derbycon, and Grrcon. Previous gigs include Google, Uber, and Bishop Fox.

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 11:00-11:50 PDT

Title: The SIEMless Hack: Rewriting Reality with Log Injection
When: Sunday, Aug 11, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

Even tools "designed to improve your security" can be ridiculously vulnerable. Paradoxically, they can actually open the door to novel types of attacks. There's a significant threat right before us, one that everyone assumed was the cornerstone of our security but overlooked: YES, your SIEM!. In this talk, I will explain how attackers become more dangerous as they grow more creative, turning our own defenses against us. I can guarantee that by the end of the talk, some of us will be saying "I wish we had never used any SIEM tools in the first place.".

In this talk, the structure of SIEM tools and hidden vulnerable points of them will be discussed, using Splunk as a primary example. This talk will include demonstrations of various attack types using the open-source offensive security tool specifically developed for this research. Prepare to be both educated and amazed as we inject fake logs, distract blue teams, and hide our activities right under their noses.

This talk will equip red teamers with a novel post-exploitation strategy to enhance their engagements, challenging blue teams with the realization that the logs they monitor minutely may not always be trustworthy.

SpeakerBio: Özgün Kültekin

No BIO available

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 11:45-12:15 PDT

Title: The Threat of Deepfakes and Synthetic Media to Election Integrity
When: Saturday, Aug 10, 11:45 - 12:15 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

How the Deepfake & Synthetic Media Framework (DSMAF) can be applied to an election context to more effectively differentiate deceptive from legitimate content and to better understand the nature of the threats posed by deceptive online content (both deepfakes and non-deepfakes). This will include a demonstration of the 2024 U.S. Presidential Election Deepfake Threat Tracker and a tutorial for how to effectively use this resource.

SpeakerBio: Dr. Matthew Canham

Dr. Matthew Canham, Co-founder of Psyber Labs and is currently the Director of Human- Machine Psychology. Dr. Canham is a former Supervisory Special Agent with the Federal

Bureau of Investigation (FBI), he has a combined twenty-one years of experience in conducting human-technology and security research. He currently holds an affiliated faculty appointment with George Mason University, where his research focuses on the cognitive factors in synthetic media social engineering and online influence campaigns. He has provided synthetic media and deepfake threat awareness training to NASA (Kennedy Space Center), DARPA, MIT, US Army DevCom, the NATO Cognitive Warfare Working Group, the Misinformation Village at DefCon, and the BSidesLV and Black Hat USA security conferences.

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 16:00-16:59 PDT

Title: The Transparency Algorithm: AI's Answer to Legal Racial and Social Inequality
When: Saturday, Aug 10, 16:00 - 16:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

The Transparency Algorithm (TTA): AI's Answer to Legal Equality is a groundbreaking initiative to dismantle the deep-rooted biases and systemic disparities that have plagued the American legal system for far too long. This revolutionary effort leverages the unparalleled power of artificial intelligence (AI) and machine learning (ML) to shine a glaring light on the injustices that have condemned generations of marginalized communities to a cycle of inequity and despair.Imagine a justice system where your fate is determined not by the content of your character but by the color of your skin, your gender, or your socioeconomic status. This is the grim reality that TTA seeks to eradicate. TTA meticulously analyzes public court case data to expose the hidden biases and discriminatory practices perpetuating injustice. This initiative doesn't just aim to reform; it seeks to revolutionize the very foundation of our legal system, bringing about the transparency and accountability that have long been overdue. At its core, TTA is a powerful tool for democratizing access to justice. Empowering citizens with data-driven insights provides a platform for informed public discourse and advocacy for systemic reform. The time for change is now, and TTA is the catalyst we need to forge a path towards a truly equitable legal landscape.

SpeakerBio: Aquarious Workman, Security Architect & Researcher

Aquarious Workman has over 15 years' experience through both military and civilian service. He began his IT career at the age of 13 assisting companies with executable security protecting application from attacks such as DLL injection and reading/writing ASM via C to be injected to manually fix unique attack vectors. He served in the United States marine corps from 2012-2017 and has held roles from Analyst to VP throughout his career. He has created many Cybersecurity programs from scratch for major corporations. He is currently the Colorado Ambassador for Blacks in Cyber (BIC), the fastest growing and national organization mentioned and referenced at President Bidens Cyber Symposium on March 2023.

Return to Index - Add to Google - ics Calendar file

MISC - Wednesday - 11:00-11:59 PDT

Title: The Unofficial DEF CON Shoot
When: Wednesday, Aug 7, 11:00 - 11:59 PDT
Where: Other / See Description

Description:

Wednesday August 7th Registration usually opens at 11am

OFFSITE: Pro Gun Vegas Address: 12801 US 95 South Boulder City, NV 89005

Return to Index - Add to Google - ics Calendar file

Title: The Value of Trust in the Open-source Software Ecosystem
When: Friday, Aug 9, 13:00 - 13:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

One year since the five-agency release of the Request for Information (RFI) on Open-Source Software Security Areas of Long Term Focus and Prioritization the U.S. government is returning to DEF CON to release an RFI Summary Report that consolidates the feedback received from the open-source software community and highlight agency-wide priorities to secure the open-source software ecosystem. In this panel, you will hear from government employees leading the charge on policy solutions towards secure open-source software and building trust with the open-source software ecosystem. In this panel, White House, the U.S. Department of Homeland Security, and Infrastructure Security Agency officials will present an overview of the Federal Government efforts in this space. The discussion will address the five priority areas addressed in the RFI, including (i) Securing Open-Source Software Foundations; (ii) Sustaining Open-Source Software Communities and Governance; (iii) Creating Behavioral and Economic Incentives to Secure the Open-Source Software Ecosystem; (iv) Improving R&D/ Innovation; and (v) Expanding International Collaboration. We look to work with you to ensure a secure, sustainable, and resilient open-source software future.

Speakers: Nasreen Djouini,Jordan Kasper,Aeva Black

SpeakerBio: Nasreen Djouini, Senior Policy Advisor at Office of the National Cyber Director (ONCD)

Nasreen Djouini is a Senior Policy Advisor at the Office of the National Cyber Director working on efforts to secure open-source software. In this role, she leads and facilitates the multi-agency working group on Open-Source Software initiative (OS3I).

SpeakerBio: Jordan Kasper, Senior Advisor for Technology and Delivery in the Office of the CIO at Department of Homeland Security

Jordan Kasper is a software engineer, speaker, tinkerer, and open source zealot. He spent much of his career in private industry building web applications for companies and organizations of all sizes. In 2017, he joined the U.S. Digital Service to help make technology better for all Americans. Since then he has worked on systems that serve millions of people and has written policies and strategies that have shaped government information technology across the board. He has developed in numerous languages from Natural on IBM mainframes to microservices in Node.js. Over the years he has spoken at over a hundred events worldwide on all things tech. He currently serves as Senior Advisor for Technology and Delivery in the Office of the CIO for the U.S. Department of Homeland Security.

SpeakerBio: Aeva Black, DHS Cyber Security and Infrastructure Security Agency

Aeva Black is an open-source hacker and international public speaker with 25 years of experience building digital infrastructure and leading open-source projects. They previously served on the OpenSSF Technical Advisory Committee, OpenStack Technical Committee, Kubernetes Code of Conduct Committee, and led open-source security strategy within the Microsoft Azure Office of the CTO. In their spare time, Aeva serves on the Board of the Open-Source Initiative and enjoys riding motorcycles and supporting the local LGBTQ+ community.

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 10:00-10:59 PDT

Title: The Village Peoples' Panel - What Really Goes On in a Village?
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

The Villages are a key part of the DEFCON experience - join this panel of staff members of the DEFCON Villages to get an inside scoop on all the intricacies of organizing a village. Topics from finding sponsors to setting up equipment to making sure everyone gets to take a break during the event - there's a whole lot that goes on behind the scenes at DEFCON villages!

Speakers: Justin,Matt Mayes,muteki,Nina Alli,Savannah "lazzslayer" Lazzara,Tom VanNorman,Jeff "The Dark Tangent" Moss

SpeakerBio: Justin, Car Hacking Village
No BIO available
SpeakerBio: Matt Mayes, Aerospace Village
No BIO available
SpeakerBio: muteki, Director at Blue Team Village
No BIO available
SpeakerBio: Nina Alli, Biohacking Village
No BIO available
SpeakerBio: Savannah "lazzslayer" Lazzara
No BIO available
SpeakerBio: Tom VanNorman, ICS Village
No BIO available
SpeakerBio: Jeff "The Dark Tangent" Moss, DEF CON Communications
No BIO available

Return to Index - Add to Google - ics Calendar file

Title: The Way To Android Root: Exploiting Your GPU On Smartphone
When: Friday, Aug 9, 14:00 - 14:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

GPU security is a vital area of mobile security highlighted both by public security research as well as by in-the-wild attacks. Due to the high complexity of the GPU software/firmware along with a widely available attack surface, issues in GPU provide strong exploitation primitives for local privilege escalation attacks by the code running in unprivileged context.

In this talk, we will focus our research on the Qualcomm Adreno GPU, which is a very popular GPU implementation in mobile devices. We will do a deep dive into Adreno GPU kernel module implementation focusing on the most recent GPU versions, reveal its complex and new attack surfaces, and discuss vulnerabilities we discovered in this component.

In total we identified 9+ exploitable vulnerabilities in Adreno GPU driver leading to kernel code execution and affecting Qualcomm-based devices using the latest GPU models. We will demonstrate the exploitation of one of the race condition issues on a fully-patched widely used Android device to obtain root privileges from zero-permission application with 100% success rate.

Android kernel mitigations such as CFI and W^X create significant hurdles for exploiting vulnerabilities in kernel to achieve code execution. Also race condition usually means unstable, low success rate. We'll explain how we overcome these challenges with a novel, generic exploit method that leverages GPU features to achieve arbitrary physical memory read/write. This technique bypasses key mitigations (CFI, W^X) and has broader implications for kernel heap buffer overflows. We will cover the technical details of the exploitation, and especially the novel generic exploit method.

We will also discuss the action items that the vendors could take to minimize the impact of this exploit method, as well as general methods to improve the overall security status of the GPU.

Speakers: Xiling Gong,Eugene Rodionov,Xuan Xing

SpeakerBio: Xiling Gong, Security Researcher, Android Red Team at Google

Xiling Gong is a Security Researcher at Google on the Android Red Team. Xiling focuses on finding and exploiting vulnerabilities in the low-level components of the Android platform and Pixel devices. Xiling has been a speaker at CanSecWest 2018, Black Hat USA 2019, Def Con 27, Black Hat Asia 2021 and Black Hat USA 2023, Def Con 31.

SpeakerBio: Eugene Rodionov, Technical Leader, Android Red Team at Google

Eugene Rodionov, PhD, is the technical leader of the Android Red Team at Google. In his current position, Eugene focuses on finding and exploiting vulnerabilities in the low-level components of the Android platform and Pixel devices. Prior to that, Rodionov performed offensive security research on UEFI firmware for Client Platforms at Intel, and ran internal research projects and performed in-depth analysis of complex threats at ESET. His fields of interest include reverse engineering, vulnerability analysis, firmware security and anti-rootkit technologies. Rodionov is a co-author of the "Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats" book and has spoken at security conferences such as Black Hat, REcon, ZeroNights, and CARO.

SpeakerBio: Xuan Xing, Manager, Android Red Team at Google

Xuan Xing is the manager of the Android Red Team at Google. For the past years, Xuan focused on finding security vulnerabilities in various low level components of Android/Pixel devices. He is passionate about software fuzzing for security

research. In Black Hat USA 2022 Xuan presented the "Google Reimagined a Phone. It was Our Job to Red Team and Secure it" talking about Pixel ABL security auditing.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 12:00-12:59 PDT

Title: The wild and wonderful world of early Microprocessors (with a focus on the 6502)
When: Saturday, Aug 10, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

This presentation will be a combination of history lesson, technical introduction, and some demonstration. The target audience are those who may never had a chance to experience early microcomputers but want to get an introduction to the world of “retro computing.

Today everyone's laptop or smartphone either run an Intel, AMD, or ARM processor. And most probably can't tell you exactly what they have or know any details of them. It’s all a black box to most. But back in the 70s and 80s, computer hobbyists & hackers knew they had a Z80, 6502, 6809, 68000 or other processor, and often knew the details and could and did program them in assembly. But while the industry has moved past the Apple II, Atari 400/800/XL/XE, Commodore 64 et al, there are still many who continue to use and enjoy these computers. Even to build and create new and exciting items for them as well as brand new systems using this old tech.

In this presentation, we will delve into microprocessor history of the 8-bit and early 16-bit systems, with a particular focus on the MOS 6502, one of the most popular microprocessors. We will touch a little on the systems that used the 6502, and take a quick look into how to program the 6502, even showing a couple of 6502-based systems. Importantly for many, we will delve into some of the resources available for those wishing to enter this world also.

SpeakerBio: Michael Brown, Security and Compliance Director at FRG Systems

Michael Brown is an information security professional and leader with years of experience in IT and information security/cybersecurity. While a security consultant advisor, he worked with clients in the healthcare, financial, manufacturing, and other sectors to assess their security programs and work with them to improve and mature their security posture. He is now Security and Compliance Director for FRG Systems, ensuring their HITRUST and SOC compliance. He is experienced with a variety of security regulations, frameworks, and standards. A seasoned speaker and presenter, he has presented at SFISSA, BSides Tampa, St Pete, and Orlando, HackMiamiCon, and ISSA International. He is an ISSA Fellow and Secretary and past president of the South Florida Chapter of ISSA and is a member of ISACA, ISC2, Infragard, and IAPP.

My first video game system was the Atari 2600, my first computer was an Atari 800XL, and second was an Atari 1040STfm. Which I still have.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 12:00-13:45 PDT

Title: The World Wide Paraweb
When: Friday, Aug 9, 12:00 - 13:45 PDT
Where: LVCC West/Floor 3/W307 - Map

Description:

Paraweb empowers people to publish and surf invisibly on a World Wide Web without the telltale traffic patterns that can betray our use of Tor and VPNs to network monitors. Paraweb is a wide-area hypermedia information retrieval initiative that combines steganography and open Web 1.0-inspired protocols to hijack and embed itself as a parasitic communications network inside existing social network websites like Tumblr, Instagram, and Reddit. Paraweb publishers can steganographically encode HTML-based, para-hyperlinked sites within innocuous media, then post those media on social network sites indistinguishably from benign content creators. Paraweb surfers can traverse these media as benign social network users, decoding the contents of para-sites as they appear normally in their searches, traversals, and feeds. Paraweb traffic is designed to blend indistinguishably with normal Web 2.0 and social network traffic, enabling Paraweb netizens to “hide in plain sight.” Paraweb’s loose and open-source combination of steganography and web-based protocols extends the hard-shell defenses of the encrypted web to the realms of deniability and stealth.

SpeakerBio: Nathan Sidles

Nathan Sidles is a person.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 11:00-11:45 PDT

Title: The XZ Backdoor Story: The Undercover Operation That Set the Internet on Fire
When: Friday, Aug 9, 11:00 - 11:45 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

On Fri, 29 Mar 2024, at exactly 08:51:26, OSS security received a message from Andres Freund, a software engineer at Microsoft, stating he had discovered a backdoor in upstream xz/liblzma that could compromise SSH servers. The open-source project XZ, specifically the liblzma library, has been compromised by a mysterious maintainer named Jia Tan, putting the entire internet at risk. Fortunately, this discovery helped us avoid the worst.

But what happened? How long has this rogue maintainer been part of the project? Who is Jia Tan? Was he involved in other projects? How does the backdoor work? And what should we learn from this?

These are questions we will attempt to answer. First, we will discuss the discovery, which is so riddled with coincidences and chance that it's hard not to think about all the ones we've missed. Then, we'll examine the process itself, from gaining trust within the project to deploying the backdoor, dissecting the operating methods and the main protagonists. We will also dive into the technical details, explaining how the backdoor is deployed and how it can be exploited.

The XZ backdoor is not just an incredible undercover operation but also a gigantic puzzle to solve. Beyond the technical background, there is a story to tell here, to capitalize on what went wrong and what we could improve.

- OSS Security Andres Freund Email: link
- My work on the XZ Backdoor: link
- Second tweet of the XZ Backdoor: link
- Additional works related to my presentation:
  - Gynvael Coldwind: link
  - link by @thesamesam@social.treehouse.systems
  - link by @eb@social.coop
  - link by @wiz_io
  - link by smx
  - link by Kaspersky
  - link by @bl4sty

SpeakerBio: Thomas Roccia, Senior Security Researcher at Microsoft

Thomas Roccia is working as a Senior Security Researcher at Microsoft and works on malware research, generative AI and threat intelligence. In addition to his work at Microsoft, Thomas also runs SecurityBreak, an online platform where he showcases his latest projects and research findings.

Thomas has travelled the world to manage critical outbreaks and has been on the front lines of some of the most well-known threats. He has tracked cybercrime and nation-state campaigns and has worked closely with law enforcement agencies.

In addition to his professional work, Thomas is a regular speaker at security conferences and is committed to contributing to the open-source community through various projects. He runs the Unprotect Project, an open malware evasion techniques database, since 2015. He is also the author of the book Visual Threat Intelligence, an illustrated guide for threat researchers. Thomas's work has been quoted by multiple media outlets around the world.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 14:00-15:45 PDT

Title: TheAllCommander 2.0
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W305 - Map

Description:

TheAllCommander is an open-source tool which offers red teams and blue teams a framework to rapidly prototype and model malware communications, as well as associated client-side indicators of compromise. The framework provides a structured, documented, and object-oriented API for both the client and server, allowing anyone to quickly implement a novel communications protocol between a simulated malware daemon and its command and control server. For Blue Teamers, this allows rapid modeling of emerging threats and comprehensive testing in a controlled manner to develop reliable detection models. For Red Teamers, this framework allows rapid iteration and development of new protocols and communications schemes with an easy to use Python interface. The framework has many tools or techniques used by red teams built in to allow out-of-the-box modeling, including emulated client browser HTTPS traffic Remote Desktop tunneling, and UAC bypass.

SpeakerBio: Matthew Handy, NASA

Matt Handy completed his BS in Computer Science at the University of Maryland, College Park (UMD) in 2010, and MS in CyberSecurity at Johns Hopkins in 2014. He has worked for NASA's Goddard Space Flight Center doing satellite ground systems development since 2009. He has specialized in secure software systems development and has helped to develop several missions over the course of his career. In his off time, he enjoys doing independent security research and creating tools like TheAllCommander to help make a more secure cyber world.

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 16:00-16:50 PDT

Title: Thinking Outside the Kube - Finding and Exploiting Command Injections in Kubernetes
When: Friday, Aug 9, 16:00 - 16:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Kubernetes is an extremely popular, open source container orchestration system, that is used by organizations large and small. Kubernetes's design philosophy leaves security to the system administrators, letting them pick and choose which security mechanisms they want to enable or disable. As such, it can leave Kubernetes deployments quite vulnerable.

In an attempt to abuse this fact, we began looking for potential exploitation avenues. Eventually, we were able to identify several vulnerabilities in different Kubernetes components that could enable a low privileged attacker to execute code, escalate privileges and exfiltrate data. We also found flaws in Kubernetes sidecar project: "gitsync". These flaws will not be patched, meaning mitigation hinges only on the awareness of security personnel.

In this talk we will go through the methodology we used to find these kinds of vulnerabilities, share our thought process on how to exploit them and show how attackers can easily execute commands with SYSTEM privileges. We will also discuss Kubernetes's design philosophy and how it can allow these types of opportunities.

SpeakerBio: Tomer Peled

No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Friday - 15:00-15:50 PDT

Title: Threat Emulation 101
When: Friday, Aug 9, 15:00 - 15:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Haven - Map

Description:

In the realm of cybersecurity, Threat Emulation is akin to a skilled wizard mastering the arcane arts of replicating real-world threats and their myriad behaviors to scrutinize the defenses of an organization. This mystical practice involves crafting Intelligence-driven scenarios, woven with the threads of reality, to mimic the nefarious maneuvers of creatures that lurk in the shadows. By summoning these simulated events, organizations can fortify their defenses, sharpening their blades against the invisible foes that threaten their digital realms.

Embark on a quest with Trey, the seasoned Threat Emulator, as he unveils the secrets of this mystical art.

SpeakerBio: Trey Bilbrey, Lead at SCYTHE Labs

Trey Bilbrey is the Lead of SCYTHE Labs, specializing in Purple Team Exercises, Threat Emulation, Critical Infrastructure, and holistic cyber operations. Trey's 15+ years of industry experience has allowed him to become an excellent educator, defender of networks, and a cultivator of cybersecurity professionals. Prior to joining SCYTHE, Trey held positions at notable organizations such as Hack The Box (HTB Academy content Developer), The Army Corps of Engineers (ICS/SCADA Penetration Testing), and a veteran of the United States Marine Corps (Defensive and Offensive Cyber Operations). Current certifications include the CISSP, GICSP, GCIP, and K>FiveFour RTAC.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-10:59 PDT

Title: Threat Hunting + Intelligence, capabilities, skills and capabilities inside the LATAM community
When: Sunday, Aug 11, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

En este panel exploraremos las capacidades y habilidades esenciales para la caza de amenazas y la inteligencia en el ámbito de la ciberseguridad, con un enfoque especial en la comunidad de América Latina. Discutiremos las técnicas y herramientas más avanzadas utilizadas en la identificación y mitigación de amenazas, así como las competencias necesarias para enfrentar los desafíos actuales en ciberseguridad. Además, analizaremos casos de estudio y compartiremos experiencias y mejores prácticas dentro de la comunidad LATAM, destacando el papel crucial que juega la colaboración regional en el fortalecimiento de nuestras defensas colectivas.

Speakers: Thiago Bordini,Mauro Eldritch,Zoziel

SpeakerBio: Thiago Bordini, Head Cyber Threat Intelligence

Thiago Bordini, Head Cyber Threat Intelligence, executive with more than 20 years of experience in the cyber intelligence market, working with analysis and prevention of cyber threats and fraud and dissemination of educational content on the subject to professionals and companies. Technical coordinator and postgraduate professor at IDESP.

Speaker at several national and international events such as YSTS, EkoParty,

H2HC, Security BSides, SANS, HTCIA, CoronaCon, 8.8 Andina and Brazil, among others.

Member of the HTCIA (High Technology Crime Investigation Association).

Member of the Security BSides Sao Paulo/Brazil organization.

SpeakerBio: Mauro Eldritch, Founder at Birmingham Cyber Arms LTD

Mauro Eldritch is an Argentine hacker, founder of Birmingham Cyber Arms LTD and DC5411 (Argentina / Uruguay). He has spoken at various events, including DEF CON (10 times). He is passionate about Threat Intelligence and Biohacking.

Mauro Eldritch es un hacker argentino, fundador de Birmingham Cyber Arms LTD y DC5411 (Argentina / Uruguay). Habló en diferentes eventos incluyendo DEF CON (10 veces). Le apasiona la Inteligencia de Amenazas y el Biohacking.

SpeakerBio: Zoziel
No BIO available

Return to Index - Add to Google - ics Calendar file

RTV - Sunday - 11:00-11:50 PDT

Title: Threat hunting like a pentester
When: Sunday, Aug 11, 11:00 - 11:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Infinity - Map

Description:

This workshop has been developed to teach participants to be one step ahead of malicious actors with the techniques they use, making use of CVE's, investigating old and new exploits, to find payloads, vulnerable directory paths, remote inclusion of files and others so you can convert them into alerts or rules in Sentinel One. We are going to first analyze some of the most used CVEs or exploits of the moment to obtain the attack vectors and later convert them into rules

SpeakerBio: Ronald Gonzalez
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Friday - 14:45-15:15 PDT

Title: Threat Modeling in the Age of AI
When: Friday, Aug 9, 14:45 - 15:15 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

How do we use the apparent magic of LLMs to help us threat model? What are the challenges? What works? What doesn't?

SpeakerBio: Adam Shostack
No BIO available

Return to Index - Add to Google - ics Calendar file

QTV - Saturday - 12:00-12:59 PDT

Title: Threat Modelling QKD
When: Saturday, Aug 10, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Much is said about QKD and its benefits and drawbacks. Even more is said about how it is, and we quote, ‘UNHACKABLE’!! We know that it is definitely susceptible to hacks, and want to invite all hackers to an open session where we will discuss attacks against QKD, both classical and quantum, and as a group start constructing a threat model that describes this technology. We will all benefit when more of us understand the real details and contexts about it! HAQ THE PLANET!

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 17:30-17:59 PDT

Title: Threat Modelling: Quantum Computers
When: Friday, Aug 9, 17:30 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

Whether you believe all the talk of Quantum Computing and its threats to classical cryptography, or are more curious for how it'll definitely stop climate change, fix AI, and give us world peace - we have identified the need to put a spotlight on the threat to quantum computers. With all the potential advantages, quantum computers will need access to some of the most highly sensitive data to carry out their quantum calculations. However, this makes them an ideal target for attackers, and we want to enumerate this threat model with YOU!

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 12:30-13:30 PDT

Title: Threats in Space: The Dangerous Rise of GNSS Attacks
When: Saturday, Aug 10, 12:30 - 13:30 PDT
Where: LVCC West/Floor 2/W235 - Map

Description:

In this 50-minute session, we will explore the critical role of Global Navigation Satellite Systems (GNSS) and the escalating cyber threats they face. GNSS technologies such as GPS, GLONASS, Galileo, and BeiDou are indispensable for providing precise positioning, navigation, and timing services across various sectors. However, these systems are increasingly vulnerable to cyber attacks. Join us to uncover disruptive techniques that threaten essential services in transportation, utilities, public safety, and finance. Don't miss the fascinating real-life case studies we'll discuss, highlighting strategies to defend against these threats.

SpeakerBio: Isabel Manjarrez, Threat Researcher (GReAT)

I am currently part of the Global Research and Analysis team (GReAT). My activities include investigating the most active threat actors, tracking their movements and analyzing new implemented techniques. With bases in telecommunications and electronics, today I have more than five years of experience performing threat intelligence tasks.

Actualmente soy parte del equipo de Global de Investigación y Análisis (GReAT). Mis actividades incluyen investigar a los actores de amenaza más activos, seguir sus movimientos y analizar nuevas técnicas implementadas. Con bases en telecomunicaciones y electrónica, hoy cuento con más de cinco años de experiencia realizando tareas de inteligencia de amenazas.

Return to Index - Add to Google - ics Calendar file

Title: Thrunting or DEATH! (A BTV Panel)
When: Saturday, Aug 10, 16:00 - 16:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

What is this Threat Hunting stuff all about? Isn't "hunting" just a cooler-sounding word for Incident Response? Why are so many new jobs opening up with Threat Hunting in the title, and how do you get the experience to land one of those jobs? Should SOC Analysts always be hunting, or is that "someone else's job?" How does CTI connect to hunting? If you have any of these questions burning in your mind, you have to come to this panel! We've got a fun and mostly sane panel of people who have different perspectives to share, and we want to hear from you, too!

Our panel of Threat Hunting practitioners will take spicy topics from our amazing moderator and the audience on topics ranging from how to thrunt to real life stories of the good, the bad and the ugly. Do you have strong opinions about whether you should call it Thrunting or DEATH? We'll ask the audience some questions, too, and you might even win a prize for your spicy take!

Speakers: Joe Slowik,Randy Pargman,Sydney Marrone,th3CyF0x,Ryan Chapman

SpeakerBio: Joe Slowik

Joe Slowik has over 15 years of experience across multiple cyber domains and problem sets. Currently Joe leads CTI functions for the MITRE ATT&CK project while also conducting critical infrastructure threat research and analysis. Previously Joe has worked in multiple roles spanning CTI, detection engineering, and threat hunting at organizations such as Dragos, Huntress, DomainTools, and Gigamon. Joe started his infosec journey with the US Navy and at Los Alamos National Laboratory.

SpeakerBio: Randy Pargman

I love helping people solve problems, especially when I get to use technology. I've been in love with programming since my grandma taught me BASIC, and if you like talking about coding, dogs, pizza, camping, or beer, I'd love to get to meet you. I especially enjoy threat hunting on endpoints, network, and email. The job I get paid for is Threat Detection at Proofpoint. In my spare time as a volunteer, I am an analyst with The DFIR Report, and I am one of the founders/organizers of DEATHCon.

SpeakerBio: Sydney Marrone

Sydney Marrone is a Principal Thrunter at Splunk. She loves all things purple, treat hunting, and pop punk.

SpeakerBio: th3CyF0x

Co-Founder of DEATHCON. 12+ years of incident response, threat hunting and threat research

SpeakerBio: Ryan Chapman

Ryan Chapman is the author of SANS' "FOR528: Ransomware and Cyber Extortion" course, teaches SANS' "FOR610: Reverse Engineering Malware" course, works as a threat hunter @ $dayJob, and is an author for Pluralsight. Ryan has a passion for life-long learning, loves to teach people about ransomware-related attacks, and enjoys pulling apart malware.

APV - Friday - 11:45-12:15 PDT

Title: Ticking SQLi
When: Friday, Aug 9, 11:45 - 12:15 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Explore the intricacies of time-based SQL injection through the lens of Operation GhostShell. This session delves into the methods used by attackers to exploit time delays for data extraction, highlighting real-world examples and the impact of these breaches on major universities. Attendees will gain a deep understanding of the technical aspects, see live demonstrations, and learn practical defense strategies to safeguard against such vulnerabilities. Perfect for security professionals seeking to enhance their knowledge of advanced SQLi techniques and mitigation.

SpeakerBio: Iggy

Igor Stepansky is a Platform Security Engineer at Axonius with two years of experience, specializing in the integration of security within DevSecOps. With a background in cybersecurity analysis in the Defense Aerospace industry, Igor expertly applies open-source tools to enhance software development security against digital threats. He champions a comprehensive security approach, emphasizing static and dynamic analysis, secrets management, and robust infrastructure as code (IaC). Igor is committed to fostering a security-conscious culture, advocating for practices that empower developers and engineers. His pragmatic and visionary perspective on cybersecurity positions him as a key figure in the field, offering actionable and forward-thinking insights.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-16:59 PDT

Title: Tinfoil Hat Contest
When: Friday, Aug 9, 10:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-D - Map

Description:

Want to protect your noggin from Taylor Swift's PsyOps plot for global domination? Have you angered our new AI Overlords, and now need to hide? Or do those alien mind control rays just have you feeling down lately? Fear not, for we here at the Tin Foil Hat Contest have your back for all of these! Come find us in the contest area, and we'll have you build a tin foil hat which is guaranteed to provide top quality protection for your cerebellum . How you ask? SCIENCE!

Show us your skills by building a tin foil hat to shield your subversive thoughts, then test it out for effectiveness.

There are 2 categories: stock and unlimited. The hat in each category that causes the most signal attenuation will receive the "Substance" award for that category. We all know that hacker culture is all about looking good though, so a single winner will be selected for "Style". We provide all contestants a meter of foil, but you're welcome to acquire and use as much as you want from other sources.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-16:59 PDT

Title: Tinfoil Hat Contest
When: Saturday, Aug 10, 10:00 - 16:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-04-D - Map

Description:

Want to protect your noggin from Taylor Swift's PsyOps plot for global domination? Have you angered our new AI Overlords, and now need to hide? Or do those alien mind control rays just have you feeling down lately? Fear not, for we here at the Tin Foil Hat Contest have your back for all of these! Come find us in the contest area, and we'll have you build a tin foil hat which is guaranteed to provide top quality protection for your cerebellum . How you ask? SCIENCE!

Show us your skills by building a tin foil hat to shield your subversive thoughts, then test it out for effectiveness.

There are 2 categories: stock and unlimited. The hat in each category that causes the most signal attenuation will receive the "Substance" award for that category. We all know that hacker culture is all about looking good though, so a single winner will be selected for "Style". We provide all contestants a meter of foil, but you're welcome to acquire and use as much as you want from other sources.

Return to Index - Add to Google - ics Calendar file

RCV - Saturday - 14:00-17:59 PDT

Title: ToolMakers Hackathon
When: Saturday, Aug 10, 14:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Unleash your creativity at the Tool Makers Hackathon, where innovation meets functionality. Collaborate with fellow hackers to design and build groundbreaking tools that push the boundaries of cybersecurity. Whether you're a seasoned pro or a budding developer, this is your chance to showcase your skills, learn from the best, and create something truly unique.

Return to Index - Add to Google - ics Calendar file

RCV - Friday - 14:00-17:59 PDT

Title: ToolMakers Hackathon
When: Friday, Aug 9, 14:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-04 - Map

Description:

Unleash your creativity at the Tool Makers Hackathon, where innovation meets functionality. Collaborate with fellow hackers to design and build groundbreaking tools that push the boundaries of cybersecurity. Whether you're a seasoned pro or a budding developer, this is your chance to showcase your skills, learn from the best, and create something truly unique.

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 17:00-17:59 PDT

Title: Top War Stories from a TryHard Bug Bounty Hunter
When: Saturday, Aug 10, 17:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Ask any top bug bounty hunter: the best part of a live hacking event is the Show & Tell; the time when the veil is lifted and we collectively revel in the ingenuity of the best finds from the competition. The goal of this talk is to give you that same experience. I will speak to you as the competent hackers that you are, not withholding the nitty-gritty technical details and the Ls along the way. Together, we'll journey through the highs and the lows of my hunts, both solo and in a Live Hacking Event context. You'll see everything from RCE to SQL injection, mass PII leakage to spying on people's homes and workplaces. You'll find some bugs mind-numbingly simple, and some bugs mind-bogglingly complex. Each bug in this talk was assigned the highest severity possible, and awarded somewhere between $10k-$60k in bounties.

SpeakerBio: Justin "Rhynorater" Gardner, Host at Critical Thinking - Bug Bounty Podcast

Yo! I'm Justin Gardner - a full-time bug bounty hunter out of Richmond, VA. I also host the Critical Thinking - Bug Bounty Podcast and advise for Caido - the latest and greatest HTTP proxy.

I'm an active member of the HackerOne live hacking event circuit (the medium through which I do most of my bug bounties) and have placed top 5 in most of the live hacking events I've attended for the past couple years. Web hacking is my sh*t, but I love all types of hacking.

Outside of hacking, I love volleyball, I love Jesus, and I love startups. Those, with a healthy dose of family and friends, keep all my free time on lock.

Return to Index - Add to Google - ics Calendar file

ADV - Saturday - 10:30-10:59 PDT

Title: Tough Adversary? Don't Blame Sun Tzu
When: Saturday, Aug 10, 10:30 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Years ago, when I started working at the NSA, I said to myself, now I can see what's really happening and what needs to be done to address our adversaries and put an end to cybercrime. Well, I was sure wrong. I worked in a few different offices and participated in hundreds of operations, only to find frustration time and time again. What happened? What was it that we just couldn't put our finger on? Yes, we were successful in addressing criminal activity. Yes, we could successfully negotiate the contested cyberspace domain. But adversarial activity kept popping up on our radar. It was Whack-A-Mole 2.0.

Was it the technologies we used? No, we had state-of-the-art capabilities. Was there a lack of technical training amongst operators? No, again, taxpayers coughed up plenty, and they got their money's worth. I concluded that it was strategy; it was philosophy. Sure, we had all the technical capabilities in the world, but we were using everything wrong.

I was in the Information Warfare Support Center. We were supposed to know what to do and how to do it! So, I started studying not only traditional but contemporary philosophy as well. I gained access to curricula in China, Russia, and the USA. This presentation informs the attendees of the adversarial philosophy taught in the military academies in China and Russia, which is taken from their curricula and papers published in various journals and practice today.

SpeakerBio: Gregory Carpenter, CSO at KnowledgeBridge International

Gregory Carpenter is the CSO of KnowledgeBridge International, a Fellow of the Royal Society for the Arts, and the National Security Agency's Operations Officer of the Year. He serves on the Board of Directors for ATNA Systems, is a Senior Advisor for ARIC, Inc., and is a Special Operations Medical Association and Military Cyber Professionals Association member. He is a former member of the Board of Advisors for EC-Council University and the International Board of Advisors for the Mackenzie Institute.

He has held various senior military and civilian positions, including COO, VP for Cyber Operations, Chief of Security Testing, Counterintelligence Division Chief, Chief of Special Space Operations, and Functional Team Lead for Electronic Warfare. He has been an epidemiological primary investigator.

Gregory is a retired army officer of 27 years, he holds a Doctorate in Public Health. He is a Certified Information Security Manager, Lean Six-Sigma Black Belt, and ISO-9000 lead auditor.

Return to Index - Add to Google - ics Calendar file

MISC - Thursday - 15:00-20:59 PDT

Title: Toxic BBQ
When: Thursday, Aug 8, 15:00 - 20:59 PDT
Where: Other / See Description

Description:

The humans of Vegas invite you to our unofficial welcome party. Whether it's your 1st or 18th time, we're still in the EXACT SAME PLACE. Join us off-Strip in the shade for a volunteer-run grill and chill.

We stock the larder with the basics: burgers, dogs, meatless delights, and all the fixin's. You procure your favorite food, drinks, and sides to keep the party going. Volunteer for setup, grill-up, or clean-up. Most of all, show up and become a part of what makes Toxic BBQ the best place to start your con.

Check out https://www.toxicbbq.org for more news, and watch #ToxicBBQ for the latest info.

Off-site at Sunset Park, Foxtail Pavilion

Return to Index - Add to Google - ics Calendar file

ICSV - Sunday - 11:00-11:50 PDT

Title: Tracking Industrial Advanced Threat Actors Who Aren't Really Advanced Just Skiddies Who Deface PLCs and Have Bad Manners: Methods and Results

When: Sunday, Aug 11, 11:00 - 11:50 PDT

Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

Industrial attacks garner a ton of attention especially from VC funded startups and government agencies who share a common goal - fundraising - I mean protecting our critical infrastructure. Threat actors around the world capitalize on geopolitical unrest and "hack" our industrial environments, posting screencaps while making wild claims. Both sides have seen an uptick in activity and I've been tracking unreal from reality. Heard of CyBeR AvEnGeRs or the CyBeR ArMy Of RusSiA ReBoRn and their terrifying water utilities hacks? (or not?) I'll deep dive into how these skiddies operate, their communication channels, claims, methods for validating claims, and general debauchery. I have receipts, will spill tea, and in this session will demonstrate for the village the methods/results of my work so everyone can see for themselves (so they can point and laugh and cry and laugh)

SpeakerBio: Ron Fabela, CEO at Infinity Squared Group (ISG)

Ron, CEO at the Infinity Squared Group (ISG), is passionate about developing practical solutions to address evolving challenges such as ransomware/extortion, expanding attack surfaces, and advanced threats against industrial control systems. With over 25 years of experience, Ron has conducted everything from exciting ICS red teaming to even more exciting ICS network cable installation, all in the quest to protect our infrastructure. The formation of ISG combines field-acquired cybersecurity expertise with a strong operational focus to safeguard critical systems.

Crocs are PPE, goats are a DHS critical sector, nothing is impossible! ²

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 16:00-16:50 PDT

Title: Tracking Real-Time Locations with Rogue WiFi Packets
When: Saturday, Aug 10, 16:00 - 16:50 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

Tracking of Wifi devices is a common requirement in the cybersecurity world from tracking rogue devices to locating bad actors. This presentation will cover a novel technique of combining passive scanning techniques with active scanning using intended behaviors within the 802.11 protocol. Passive scanning is available through software in suites such as Kali, or in tools like a Pineapple, with the disadvantage of being only as fast as the target is willing to send packets. Active scanning has been traditionally relegated to only devices attached to the same Access Point or other, expensive gadgets while gaining the advantage of eliciting responses on command. Using a technique based on Wifi-Polite packets, cheap ESP32s can be leveraged to gain the advantages of active scanning without the requirement of being connected to the same Access Point. The software code operating this powerful combination of active and passive scanning on an inexpensive platform will be publicly released. Attendees will have a clear understanding of the technology, be given the knowledge and code to implement it themselves, and understand the future implications of using devices like this in a cooperative mesh to track targets in real time.

SpeakerBio: Mikey Awbrey

Having worked for years as an engineer across multiple industries, such as satellite, radar, and UAV, Mikey has a unique, systems based approach to his work. This has lead to a number of critical zero days, and novel applications of hacking techniques. His most recent years have been working as a penetration tester for government and commercial clients alike.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 13:00-13:45 PDT

Title: Transforming AppSec: Protecting 'Everything as Code' & Emerging Tech
When: Saturday, Aug 10, 13:00 - 13:45 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

The continuous adoption of emerging technological trends like Mobile, IoT, Cloud, Blockchains, and now GenAI has transformed application security from simple threat modeling and SAST/DAST scans to comprehensive proactive prevention and real-time detection of security anomalies. This panel will discuss the dynamic nature of AppSec as the lines between traditional infrastructure and cloud environments blur. We will explore the importance of maintaining a comprehensive security posture within 'everything as code' ecosystems, emphasizing proper configuration and secret management to secure infrastructure effectively.

Speakers: Kunal Bhattacharya,Sara Attarzadeh,Shahar Man,Trupti Shiralkar

SpeakerBio: Kunal Bhattacharya

A Security Leader, Organization builder and mentor who helps organizations build robust Cyber defense and detection capabilities. I do this by building Secure SDL processes and machination encapsulating Shiftleft strategy, SecDevOps, Cloud and Penetration testing. My prior experience in all phases of Application development, System and database administration and Quality engineering helps me in building lasting relationships with peers in engineering and product organizations and working towards shared security goals.

SpeakerBio: Sara Attarzadeh

TBA

SpeakerBio: Shahar Man

Passionate about building and leading teams, I have successfully grown Engineering and Product teams from scratch, leveraging Agile methodologies. My focus lies in Application and Cloud Security, advocating for context-driven AppSec decisions.

SpeakerBio: Trupti Shiralkar

Trupti has 18 years of diverse experience, leading security and privacy initiatives in Fortune 500 companies and dynamic startups. Currently she is exploring data security and privacy space as part of her stealth mode startup “TrueNil”. Her journey is marked by cultivating high-performing teams, pioneering product security and privacy engineering strategies, and instilling a progressive mindset. A seasoned public speaker and product security leader, she passionately imparts her insights to drive positive security impacts and mitigate organizational risks. Notably, she holds a patent for a secure and anonymous electronic polling solution.

Return to Index - Add to Google - ics Calendar file

QTV - Friday - 15:00-15:59 PDT

Title: Trapped Ion Quantum Computing Systems - Behind The Scenes: from the physics to control electronics
When: Friday, Aug 9, 15:00 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-01 - Map

Description:

In this two-part presentation, we will explore the workings of trapped-ion quantum computers. The first part provides an introduction to the fundamental concepts of quantum computation, as well as the scientific principles behind implementing these concepts with lasers and trapped ions. The second part delves into the practical aspects of trapped-ion quantum computing by following a quantum circuit through the process of compilation and execution by control electronics.

Speakers:Daiwei Zhu,Rick Altherr

SpeakerBio: Daiwei Zhu

Daiwei Zhu is a quantum application researcher at IonQ, having joined the team following the completion of his PhD in experimental ion trap quantum computing. His current research focuses on quantum algorithms, quantum machine learning, reinforcement learning, and optimizing quantum circuit compilation.

SpeakerBio: Rick Altherr

Rick Altherr is a full stack engineer having worked on everything from ASIC design to user experience (UX) in systems ranging from embedded to hyperscale. Their career has kept them close to the hardware software boundary, primarily working on computer systems at Apple, Google, and Oxide Computer. After a multi-year detour through firmware security, Rick is now designing instruction sets, microarchitecture, and real-time embedded control systems for trapped-ion quantum computers at IonQ.

Return to Index - Add to Google - ics Calendar file

CPV - Friday - 11:00-11:30 PDT

Title: Travel Better: Expedient Digital Defense
When: Friday, Aug 9, 11:00 - 11:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Expedient Digital Defense focuses on using free and readily available applications, or recommending paid-for commercial apps and tools that have proven records of credibility, to make our devices and online presence less harmful to us. We will follow a typical traveler in the United States, with some experiences drawn from overseas travel.

The talk stresses the value of Operational Security (OPSEC), and the mindset of seeing every piece of communication through the eyes of your adversary. The intent is to make people think twice before revealing anything considered sensitive, even if using the latest and greatest encryption. The surveillance economy and ever-present data collection in our modern world demand better awareness of how our digital world works. We'll discuss examples like invasive social media collection, foreign influence on public perception, data insecurity putting users in danger, and advertising models based on location and click tracking.

Finally, the take-away is knowing the tools and tech available, and being able to select those which fit your needs, if at all. Most of the time, one mitigation isn't enough, and several need to be emplaced to achieve proper defense in depth, in case one solution fails. Even if no technical solutions are put in place, the user will have that "red team" mindset and awareness that calibrates better judgment over technical solutions, and promotes OPSEC and rational thinking for security rather than blindly depending on apps and gadgets.

SpeakerBio: Grey Fox

Grey Fox, the callsign assigned to him by a DHS colleague, recently retired from the U.S. military after 20 years of service as an intelligence analyst, language analyst, digital network intelligence targeter, cyberspace mission leader, and digital defense education program leader. Having deployed eight times supporting front line combat teams, his experience ranges from offensive cyberspace operations planning and execution to military information support operations. Along the way, Grey Fox acquired multiple creds, including GCTI, GASF, GAWN, and CWNA. He currently instructs Digital OPSEC at the U.S. Army Security Cooperation Officer course and the U.S. Air Force Research Lab, as well as SDR foundations and Wi-Fi hacking at the U.S. Army Signal School.

Return to Index - Add to Google - ics Calendar file

XRV - Friday - 11:00-12:59 PDT

Title: Trip Through Reality XR for Performances Masterclass with the Glad Scientist
When: Friday, Aug 9, 11:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-01-06 - Map

Description:

The Glad Scientist will share their experiences and techniques for building out immersive performances, with a specific focus on their unique use of XR and generative AI in their process. Expect VR modular synthesis, weird generative AI hacks, and a lot of talk about breaking things in the name of creativity! This session is beginner-friendly, and attendees are welcome to follow along and test these techniques, or to listen and ask questions.

SpeakerBio: The Glad Scientist

The Glad Scientist is a Barcelona-based media artist, performer, and professor who has integrated XR into their artistic process since 2017. Their work has been seen in worldwide venues, galleries, and festivals including DreamHack, Ars Electronica, Sonar+D, and Venice Biennale. Commercially, they have worked on immersive projects for several J-Rock bands, Under Armour, and Universal Studios' Super Nintendo World.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 14:30-15:15 PDT

Title: Troll Trapping Through TAS Tools - Exposing Speedrunning Cheaters
When: Saturday, Aug 10, 14:30 - 15:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 2 - Map

Description:

Trolls cheating in video games by passing Tool-Assisted Speedruns off as human effort break leaderboards and stifle speedrunners. Why do they do it when they could make a cool game hack or TAS to show off their work, and how do you trap these trolls? The answer is to use their own tools against them, often with popcorn bucket worthy results like taking down Guinness World Records. From a TASVideos member taking on 1980's Dragster cheat Todd Rogers, a passing mention of Billy Mitchell, and the TASBot team investigating Super Mario Maker shenanigans, this talk covers several notable cheating incidents and concludes with a systematic takedown of a troll that chilled the Diablo speedrunning community for more than a decade.

This talk includes several investigations I have been a part of in some capacity and will ultimately include additional references in the coming months; I've broken the references out by game, presented in Markdown format like the rest of this document:

Dragster

- Submission #5517: Omnigamer's A2600 Dragster in 00:08.49
- A2600 Dragster by Omnigamer in 00:08.49
- Submission #5876: MrWint & Omnigamer's A2600 Dragster in 00:08.39
- A2600 Dragster by MrWint, Omnigamer in 00:08.39
- Omnigamer's Dragster simulator model
- Dragster optimal sequence project by esnard
- Investigation into optimal Dragster play by MrWint
- TASBot beats Dragster in 5.57 (console verification of Omnigamer's TAS)

Super Mario Maker

- Inside TASBot's semi-secret, probably legal effort to control the Nintendo Switch
- The *Super Mario Maker* community faces its final boss
- *Super Mario Maker*'s "final boss" was a fraud all along
- How to cheat at *Super Mario Maker* and get away with it for years
- Trimming the Herbs TAS attempts
- Trimming the Herbs has been Beaten

Diablo

- Speed Demos Archive Diablo page
- Groobo's 2009 Diablo speedrun submission video
- Speed Demos Archive Diablo run review
- Guinness World Records Diablo entry
- Devilution Diablo decompiliation
- DevilutionX Diablo decompiliation
- Diablo MapGen

SpeakerBio: Allan "dwangoAC" Cecil, Founder and Leader at TASBot Online Community

dwangoAC (Allan Cecil) is the founder and leader of the TASBot online community and Senior Ambassador on staff of TASVideos.org. He is a published journal author, patent holder, and unflappable presenter with talks at DEF CON, GeekPwn, Thotcon, May Contain Hackers, and other hacker conferences. dwangoAC uses his combined hacking interests for good at charity events like Games Done Quick to entertain viewers with never-before-seen glitches in games, with event content he's led raising more than $1.5m for various charities.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 12:00-12:50 PDT

Title: Tunnel Vision: Exploring VPN Post-Exploitation Techniques
When: Saturday, Aug 10, 12:00 - 12:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Side Winder - Map

Description:

We all heard this story before - a critical vulnerability is discovered in a VPN server. It's exploited in the wild. Administrators rush to patch. Panic spreads across Twitter.

Attackers have long sought to exploit VPN servers - they are accessible from the internet, expose a rich attack surface, and often lack in security and monitoring. Historically, VPNs were primarily abused to achieve a single objective: gaining entry into internal victim networks. While this is evidently very valuable, control over a VPN server shouldn't solely be seen as a gateway to the network, and can certainly be abused in various other ways.

In this talk, we will explore VPN post-exploitation - a new approach that consists of different techniques attackers can employ on the compromised VPN server to further progress their intrusion. To demonstrate this concept, we will inspect two of the most common VPN servers on the market - Ivanti Connect Secure and Fortigate, and show how an attacker with control over them can collect user credentials, move laterally, and maintain persistent access to the network.

We will conclude by detailing best practices and principles that should be followed by security teams when using VPN servers to reduce the risk from post-exploitation techniques.

SpeakerBio: Ori David

No BIO available

Return to Index - Add to Google - ics Calendar file

CHV - Friday - 14:00-14:30 PDT

Title: UDSonCAN Attacks: Discovering Safety-Critical Risks by Fuzzing
When: Friday, Aug 9, 14:00 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Some diagnostic services in UDSonCAN that could affect driving should be disabled while driving and protected by authentication mechanisms such as SecurityAccess. However, without these security measures, attackers can cause a serious safety risk to the driver using only diagnostic messages. In this talk, we introduce UDSonCAN attacks discovered through fuzzing and describe their countermeasures. These attacks can cause a moving car to suddenly stop or a stationary car to suddenly acceleration with just simple diagnostic messages. We discovered these vulnerabilities in the latest electric vehicle model and have prepared a demo.

Speakers: Jonghyuk Song,Seunghee Han,Soohwan Oh

SpeakerBio: Jonghyuk Song
No BIO available

SpeakerBio: Seunghee Han, Automotive Engineer and Security Tester at Autocrypt Engineering

Seunghee Han is an automotive engineer and security tester at Autocrypt Engineering team. She is mainly working on fuzzing test and issue analysis on the in-vehicle networks, such as CAN/CAN-FD, UDSonCAN, and Automotive Ethernet. Also, she has designed the requirements of automotive security test solutions.

SpeakerBio: Soohwan Oh
No BIO available

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 17:00-17:59 PDT

Title: Under the Hood: Incident Response at High Speed (A BTV Panel)
When: Saturday, Aug 10, 17:00 - 17:59 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

This talk with dive into:
• The speed of threats coming at us today, and how teams manage burnout and back to back calls.
• How the incident response landscape is changing.
• Do AI and ML change incident response?
• How do the recent takedowns performed by LEs affect IR?

In an era where cyber threats evolve at breakneck speed, the ability to respond swiftly and effectively has never been more critical. Join us for "Under the Hood: Incident Response at High Speed," where we'll delve into the high-stakes world of incident response and explore how teams are adapting to the relentless pace of modern threats. Discover the innovative ways AI and machine learning are transforming our defensive strategies and hear expert insights on the shifting landscape of incident management. We'll also examine the recent high-profile takedowns of droppers, C2s, and ransomware leak sites to determine whether these efforts are truly mitigating long-term risks or if we need a new approach to stay ahead. Your pit crew panel consists of leaders and practitioners from across industries and the globe discussing the latest and greatest in the world of Incident Response. Don't miss this opportunity to gain cutting-edge knowledge and strategies for navigating the evolving cyber threat landscape.

Speakers: Angelo Violetti,David Zito,Nicole Beckwith,Shelly Giesbrecht

SpeakerBio: Angelo Violetti, Incident Response and Digital Forensics consultant at SEC Consult

Angelo is an Incident Response and Digital Forensics consultant with four year of experience in this field. He works for SEC Consult, a cyber security company based in the DACH region, and he supports the DFIR Report by writing blog posts and providing actionable Threat Intelligence.

He has also experience in offensive projects such as penetration tests and red team engagements.

SpeakerBio: David Zito, VF Corp

David is a reformed Fed who spent the bulk of his career in the defense and federal sectors. Now he leads incident response operations for VF Corp, a leader in the fashion and retail industry. David is passionate about combatting burnout in the DFIR field and DFIR in general. He previously worked at CISA where he led national incident response operations. David is 100% a crazy cat person and loves all things nerd culture. He loves sharing battlefield stories and talking about the growth of DFIR and what the future holds. So come find him, say hi, and swap stories!

SpeakerBio: Nicole Beckwith

Meet Nicole Beckwith, a dynamic DFIR guru and former law enforcement officer who’s now leading Threat Operations for Kroger. Nicole’s expertise in cyber security is only rivaled by her enthusiasm for pineapple on pizza—because it definitely belongs there! When she’s not protecting the digital aisles or soldering tech innovations, Nicole is a proud Star Wars nerd and an aficionado of Vanilla Ice’s tunes (a fun fact she flaunts with the rapper’s follow on X). With a mix of hands-on experience, pop culture savvy, and a fascinating challenge coin collection, Nicole brings a unique and engaging perspective to every discussion.

SpeakerBio: Shelly Giesbrecht

A long-time admirer of smart people, Shelly works hard to surround herself in people she can learn from. This is particularly easy to do in her day job as a Director (IR) for CrowdStrike Services. She is frequently found wearing a bow-tie and some form of red sneakers. Her favourite role in life is dog mama, and she'll talk your ear off about her Lego collection if you are brave enough to ask.

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 14:45-15:30 PDT

Title: Understanding Cognitive Warefare in a Geopolitcal Context
When: Saturday, Aug 10, 14:45 - 15:30 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

We are living through a secular (once in a lifetime) crisis period that presents an existential risk to democracy, both at home and abroad. There are various underlying sociological, geopolitical and economic forces that give rise to a crises of this magnitude. How are authoritarian actors exploiting this to weaken the liberal democratic order? How can these dynamics help us create a frame to better understand the nature of Cognitive Warfare? Our liberal democratic system is under increasing levels of attack. Who are the internal and external threat actors behind this? Are they working together? Our liberal democratic system is under increasing levels of attack. Who are the internal and external threat actors behind this? Are they working together? The terms disinformation and misinformation are often used to describe cognitive warfare influents (instances of influence used in a CW campaign), but these terms can also limit our ability to detect and defend. Let's explore a model of Cognitive Warfare that helps us understand the broad range of tactics being used as well as who is being targeted and how.We will also explore how Cognitive Warfare can complement other domains of conflict and how CW has even been used as part of kinetic combat operations. What are some of the natural asymmetries when CW is being used in conflicts between authoritative and democratic systems? Join us as we work to grow and model our understanding this new and critical domain of conflict.

SpeakerBio: Constantine Nicolaidis

Constantine leads a Risk Management practice that focuses on securing U.S. privately owned critical infrastructure. Over the last decade he has leveraged his expertise in security and data-based product development to create tools for security professionals. Constantine has also spent the last 5 years developing a geopolitical modeling system to help forecast and describe the nature of political and social crises. He advises various security groups on the nature of modern multi-domain warfare with an emphasis on the cyber and cognitive domains. Constantine holds a Master's Degree in Human-Computer Interaction from the Carnegie Mellon School of Computer Science and is currently enrolled in the Master's in Cybersecurity Degree program at the SANS Technology Institute.

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 14:00-14:45 PDT

Title: Understanding the Role of Secretary of States in Elections
When: Saturday, Aug 10, 14:00 - 14:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

This talk will cover the role that Secretaries of State's offices play in Elections. This talk with also dive into the election processes that the State of NH follow and all the ways they do whatever they can to keep elections secure. It is a rare opportunity to hear directly from a Secretary of State the roll they play in national elections. This talk will allow audiences to have a better understanding of how these processes work and why Secretary of States play such a critical role in elections.

SpeakerBio: Dave Scanlan, Secretary of State at New Hampshire

David M. Scanlan (born June 14, 1956) is an American politician and election official serving as the 54th secretary of state of New Hampshire. A Republican, he assumed office as acting secretary of state upon the resignation of Bill Gardner on January 10, 2022. He was elected to a new two-year term as secretary of state by the New Hampshire General Court (state legislature) on December 7, 2022. He previously served as deputy secretary of state, since 2002[and served in the New Hampshire House of Representatives from 1984 to 2002, becoming majority leader.

Return to Index - Add to Google - ics Calendar file

Title: Underway to Identifying Commonalities of Cybersecurity Incidents in the Maritime Transportation System
When: Saturday, Aug 10, 15:00 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The purpose of this study is to identify commonalities in cybersecurity incidents in the maritime transportation system (MTS). For this exploratory study, the researcher expanded upon their previous research into identifying commonalities in cyberattacks by analyzing documents to identify trends concerning all cybersecurity incidents in the civilian and military MTS components. The MTS can use identified commonalities from the expanded study, including all cybersecurity incidents impacting the civilian and military aspects, to make better informed decisions on cybersecurity threats and appropriate measures. In addition to the Diamond Model of Intrusion Analysis and the information security triad—Confidentiality, Integrity, or Availablity (CIA), this study incorporates additional cybersecurity concepts, such as the Parkerian Hexad and the MITRE ATT&CK framework, to provide more granularity to commonalities identifying in previous research.

SpeakerBio: Rebecca J. Rohan

Rebecca Rohan has over 15 years of experience in cyber threat intelligence and information security and is currently completing her Doctor of Science in Cybersecurity at Marymount University in Arlington, VA. She has been a certified SANS Global Industrial Cyber Security Professional (GISCP) since January 2016. Her main academic research areas are maritime cybersecurity, cybersecurity education, cybersecurity intelligence, and diversity in cybersecurity.

Return to Index - Add to Google - ics Calendar file

CLV - Sunday - 12:20-12:40 PDT

Title: Unexpected Leaks in AWS Transit Gateways
When: Sunday, Aug 11, 12:20 - 12:40 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

Engineers can carefully build their networks, designing the traffic flow explicitly through well constructed controls, even following design best practices from the CSP themselves, only to be let down by unexpected subtleties in the exact way certain technologies operate.

In this talk, we will take a look at just such a case study concerning Transit Gateways (TGW) in AWS, where security consultants were able to communicate freely across an apparent network boundary. We will review how TGWs are attached to subnets, and how the documentation implies they should operate. Then we will examine why NACLs appeared to be having no effect on blocking traffic, and allowed an effectively flat network between two peered accounts.

This case study will demonstrate the importance and effectiveness of practical testing, either internally by the developers or with an external reviewer, in confirming – or in many cases quite the opposite – that the operation matches the design aims. It isn't always easy to find that leak, but if there is a puddle of water on the floor then at least you know you need to start looking for the flaw. This talk will show through the TGW case study and a few other examples how we noticed the puddle, how we found the leak, how it was fixed, and how hopefully the same leak won't spring twice.

SpeakerBio: William Taylor

Security consultant with a background in embedded engineering and DevOps, which has lead to an interest in mobile, Cloud, and Kubernetes security. I used to make things work; now I break things, professionally and ethically.

Return to Index - Add to Google - ics Calendar file

Title: Unlocking Hidden Superpowers: Neurodiversity in Infosec
When: Saturday, Aug 10, 16:05 - 17:05 PDT
Where: Virtual

Description:

Are you ready to embark on a journey that celebrates uniqueness, innovation, and untapped potential? It's time to shine a light on Neurodiversity and what that means to Information Security.

1. The Power of Neurodiversity:

Imagine a world where different brains aren't seen as deficits but as diverse strengths. Neurodiversity embraces the beautiful mosaic of human minds, from ADHD to autism and beyond. Xavier will unravel the superpowers hidden within neurodivergent individuals—like visual hypersensitivity, out-of-the-box thinking, and encyclopedic knowledge. These aren't just buzzwords; they're game-changers for the Infosec field.

1. Success Stories and Real Impact:

Brace yourself for success stories that defy convention. JPMorgan Chase's neurodiverse hires outperform their peers by leaps and bounds. Productivity spikes, retention soars, and innovation thrives. Ultra Testing, an IT company with 75% neurodiverse staff, proves that inclusion isn't charity—it's smart business. Their mantra? "Staffing fantastically capable talent who just haven't had a fair shot before."

1. Creating an Inclusive Future:

Xavier won't stop at inspiration; he'll equip you with actionable steps including: How to Revisit Hiring Processes, Adapting the Environment, Tailored Career Journeys

1. Be Part of the Movement:

Whether you're a hacker, an individual seeking help, or just a cat lover (yes, there's a slide for that!), this presentation is your invitation to change the narrative.

So mark your calendar, grab your virtual seat, and let's celebrate neurodiversity—one mind at a time. Remember, the rising tide lifts all boats. Join us, learn, and be part of a more inclusive future! Don't miss out—this isn't your typical tech talk. It's a revolution waiting to happen. See you there!

SpeakerBio: Xavier "rubix1138" Ashe, Senior Vice President, Cyber Operations and Technology at Truist

Xavier Ashe is currently a Senior Vice President in Truist's Cyber Operations and Technology division where he was awarded the Truist Performance Award. He is Chairman of the Board for the Technology Association of Georgia (TAG) Information Security Society. Xavier is a Georgia Institute of Technology alumnus and has over 30 years of leadership experience in information security, working for various vendors and consulting firms including IBM, Gartner, and Carbon Black. Xavier was the first hire at the startup Drawbridge Networks, where he was instrumental in bringing the first microsegmentation solution for servers and workstations to market. Mr. Ashe has plenty of war stories, including the first DDOS attack ever, Target, Sony, Aramco, [REDACTED], and others. Xavier is an accomplished speaker and has presented at many security conferences including DefCon, BlackHat, RSA, BSides, Splunk .conf, SANS, and others.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 11:40-12:10 PDT

Title: Unlocking the Gates - Understanding Authentication Bypass Vulnerabilities
When: Saturday, Aug 10, 11:40 - 12:10 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

During the session, I will present an extensive array of over 15 distinct techniques and vulnerabilities that can be exploited for authentication bypass or account takeover. Some of the vulnerabilities I will cover include Session Puzzling, Session Fixation, Rate Limit Bypasses, Broken Brute-Force Protection, 2FA/OTP Misconfigurations, HTTP-Parameter Pollution, PHP Type Juggling, and many more. These insights will provide attendees with a comprehensive understanding of the various methods used by attackers to compromise authentication mechanisms and take control of user accounts.

SpeakerBio: Vikas Khanna

I specialize in Web Application and API Security Assessments. I have worked with industries spanning Finance, E-Commerce, Employee Management, Food, Beverages, and Fitness. I have a track record of successful bug bounty hunting and have identified major security flaws in prominent organizations such as Apple, Google, Microsoft, Oracle, Verizon, Sony, IBM, Intel, Nokia, and ING Bank.

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 10:00-10:20 PDT

Title: Unlocking the Gates: Hacking a secure Industrial Remote Access Solution
When: Sunday, Aug 11, 10:00 - 10:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 4 - Map

Description:

Industrial VPN gateways play a crucial role in operational technology by enabling secure remote access to systems within industrial networks. However, their importance goes hand in hand with increased security risks, as their architecture makes them lucrative targets for threat actors. Over the years, we have seen such devices being used in various industrial environments, which underlines their widespread use in critical infrastructures.

This talk is about a security analysis of a widely used industrial remote access solution. We will dive deep into and expose various vulnerabilities. This includes rooting the device, bypassing hardware-based security mechanisms such as the use of a hardware security module, and reverse engineering software and firmware. Ultimately, we will show how various identified vulnerabilities allowed us to hijack remote access sessions, creating significant security risks.

SpeakerBio: Moritz Abrell, Senior IT Security Consultant and Penetration Tester at SySS GmbH

Moritz Abrell is an experienced IT security expert who has been passionate about the field since his early days.

As a Senior IT Security Consultant and Penetration Tester for the Germany-based pentest company SySS GmbH, he specializes in the practical exploitation of vulnerabilities and advises clients on how to remediate them.

In addition, he regularly conducts security research and has a keen interest in delving deep into soft-, hard- and firmware. His research has been presented at various national and international IT security conferences such as DEFCON, BlackHat USA, HackCon, NoHat, Hacktivity, etc.

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 10:45-11:30 PDT

Title: Unmasking Shadows: Strategies on Hunting Ransomware Groups
When: Saturday, Aug 10, 10:45 - 11:30 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

In the modern world of cybersecurity threats, ransomware groups pose a significant challenge to organizations worldwide. This talk, tailored for cybersecurity students and professionals, delves into practical techniques for tracking and dismantling these elusive adversaries. Attendees will explore methods such as monitoring the latest ransomware attacks, engaging with ransomware blogs on the dark web, and reaching out to victims to gather firsthand insights into the operations of these malicious entities. By combining these strategies, participants will gain a comprehensive understanding of how to unmask and combat ransomware groups, bolstering their defenses against this pervasive threat.

SpeakerBio: R.J. McCarley, Principal Security Researcher
No BIO available

Return to Index - Add to Google - ics Calendar file

CLV - Friday - 14:00-14:30 PDT

Title: UnOAuthorized: Discovering the path to privilege elevation to Global Administrator
When: Friday, Aug 9, 14:00 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-09-01 - Map

Description:

For customers of Microsoft 365 and Azure, obtaining the role of Global Administrator (GA) is every attacker's dream - it is the Domain Administrator of the cloud. This makes Global Administrator every organization's nightmare of being owned by a threat group or hacker. Luckily, well-defined role-based access control and a strict application consent model can severely limit who gets their fingers on Global Administrator - or does it?

This talk explores a novel discovery that resulted in privilege elevation to Global Administrator in Entra ID (Azure AD). Part conversation about the research background, part discussion of the foundational components involved, this talk will walk step-by-step through the path to privilege elevation, and owning Global Admin.

SpeakerBio: Eric Woodruff

Throughout his 24-year career in the IT field, Eric has sought out and held a diverse range of roles, including technical manager in the public sector, Sr. Premier Field Engineer at Microsoft, and Security and Identity Architect in the Microsoft Partner ecosystem. Currently he is a Sr. Cloud Security Architect working as part of the Security Research team at Semperis. Eric is a Microsoft MVP for security, recognized for his expertise in the Microsoft identity ecosystem. Outside of work, Eric supports the professional community, providing his insights and expertise at conferences, participating on the IDPro Body of Knowledge committee, and blogging about Entra and related cloud security topics.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 15:30-16:15 PDT

Title: Unsaflok: Hacking millions of hotel locks
When: Saturday, Aug 10, 15:30 - 16:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Electronic hotel locks have been in use for over three decades, and have become an integral part of the hospitality sector. Las Vegas has over 150.000 hotel rooms, many of which use an RFID based electronic lock for access control. Most hotel guests rely on these locks to safeguard personal belongings and to protect their personal safety. However, some of these long-deployed locks have never been publicly scrutinized by the research community.

This presentation covers the discovery of vulnerabilities affecting three million dormakaba Saflok locks. The Saflok system relied on a proprietary key derivation function for its MIFARE Classic cards and a proprietary encryption algorithm for the card contents. Reverse engineering the Saflok system allowed us to forge valid keycards. After reading a single, low privilege, guest card we are able to create a pair of forged key cards that allow us to deactivate the deadbolt and open any room at the property.

We reported these vulnerabilities to dormakaba in September of 2022, as part of this presentation we will discuss the responsible disclosure and mitigation processes. Additionally, we will demonstrate how you can determine if your own hotel room has been patched to help ensure your personal safety.

1. My Arduino can beat up your hotel room lock - Onity locks - Cody Brocious - Blackhat 2012
2. Ghost In The Locks: Owning Electronic Locks Without Leaving A Trace - Vingcard locks - Tomi Tuominen and Timo Hirvonen - HITBGSEC 2018

Speakers: Lennert Wouters,Ian Carroll

SpeakerBio: Lennert Wouters, Security Researcher, Computer Security and Industrial Cryptography (COSIC) at KU Leuven University

Lennert Wouters is a security researcher at the Computer Security and Industrial Cryptography (COSIC) research group at the KU Leuven University in Belgium. Lennert's main research interests cover hardware security for embedded systems and physical attacks.

SpeakerBio: Ian Carroll, Independent Security Researcher

Ian Carroll is an independent security research and founder of Seats.aero. Ian's main research interests involve application security, especially in the travel industry.

Return to Index - Add to Google - ics Calendar file

BBV - Saturday - 16:00-17:30 PDT

Title: Unveiling Vulnerabilities: A Comprehensive Guide to Bug Bounty Recon
When: Saturday, Aug 10, 16:00 - 17:30 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

In the rapidly evolving landscape of cybersecurity, effective reconnaissance is the cornerstone of successful bug bounty hunting. This presentation will guide you through identifying, enriching, and prioritizing targets before any scanning occurs, emphasizing the importance of uncovering "unknown unknowns." We will cover the use of tools like subfinder and amass for asset discovery, followed by httpx for extracting relevant data such as titles and ports. Prioritization will be discussed to focus efforts on high-potential targets, including those requiring sign-in. Once prioritized, we'll move to scanning, employing advanced techniques to uncover hidden files and functionalities, targeting both known vulnerabilities and the elusive "unknown unknowns." Finally, we'll focus on exploiting discovered functionalities, equipping you with the skills to uncover and exploit weaknesses. Join us to enhance your bug bounty hunting capabilities with a methodical approach to reconnaissance and exploitation, ensuring no stone is left unturned in your quest for vulnerabilities.

Speakers: Dhiyaneshwaran Balasubramaniam,Prince Chaddha,Tarun Koyalwar

SpeakerBio: Dhiyaneshwaran Balasubramaniam, Nuclei Template Engineer at ProjectDiscovery.io

Dhiyaneshwaran is a Nuclei Template Engineer at ProjectDiscovery.io, crafting Nuclei templates for trending exploits and CVEs. With over 1350 templates written, he leads the Nuclei-Templates leaderboard. In his free time, he engages in bug bounty hunting and develops unique reconnaissance methodologies. He is also an active speaker and organizer in the cybersecurity community, contributing to Null Chapter, OWASP Local Chapters, and BSides Chapters.

SpeakerBio: Prince Chaddha, ProjectDiscovery

Prince Chaddha leads the nuclei-templates project at ProjectDiscovery. With over a decade of experience in web application security, bug bounties, code auditing, and pentesting across various domains, including network, API, mobile, cloud, and infrastructure security. He actively writes about DevSecOps and cloud security, including AI, open-source, and blockchain security.

SpeakerBio: Tarun Koyalwar, Go developer at ProjectDiscovery

Tarun is a Go developer at ProjectDiscovery, where he maintains and contributes to open-source projects such as Nuclei, Cvemap, Katana, and Subfinder. He specializes in developing and contributing to automation tools for bug bounty hunting, with a focus on large-scale automation and fuzzing techniques. Alongside his development work, Tarun has hands-on experience as a part-time bug bounty hunter. He is passionate about discovering and refining techniques for automating bug bounty experience

Return to Index - Add to Google - ics Calendar file

Title: US and International Public Cyber Policy 101
When: Friday, Aug 9, 10:00 - 11:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

The session will provide an overview of the current themes and topics being explored by US and International policymakers. It will help provide clarity into the landscape of cyber public policy, highlighting the need for governments around the world to align on policy development and intervention. It will help establish a baseline of knowledge on what's happening in global cyber policy for those wanting to get up to speed, and will help set the scene for many of the policy discussions to come throughout DEF CON.

Speakers: Harley Geiger,Adam Dobell,Cassie Crossley

SpeakerBio: Harley Geiger, Venable

Harley Geiger is a legal and public policy specialist with deep experience in vulnerability management and disclosure. He leads the Hacking Policy Council, a group of senior executives with policy, business, and technical expertise in vulnerability management.

SpeakerBio: Adam Dobell

Adam Dobell has extensive experience in cybersecurity and international policy, principally in the Indo-Pacific. Prior to joining Venable, Adam served as the first secretary for the department of home affairs at the Embassy of Australia in Washington DC, where he engaged with officials at the White House and congressional and industry stakeholders to further Australia's national security interests. He also represented the Australian Government in multilateral groupings including the Asia Pacific Economic Cooperation, the International Counter Ransomware Initiative, and the Quad.

SpeakerBio: Cassie Crossley, Vice President, Supply Chain Security, Cybersecurity & Product Security Office at Schneider Electric

Cassie Crossley, Vice President, Supply Chain Security in the global Cybersecurity & Product Security Office at Schneider Electric, is an experienced cybersecurity technology executive in Information Technology and Product Development and author of "Software Supply Chain Security: Securing the End-to-End Supply Chain for Software, Firmware, and Hardware." She has many years of business and technical leadership experience in supply chain security, cybersecurity, product/application security, software/firmware development, program management, and data privacy. Ms. Crossley has designed frameworks and operating models for end-to-end security in software development lifecycles, third party risk management, cybersecurity governance, and cybersecurity initiatives. She has an M.B.A. from California State University, Fresno, and her Bachelor of Science degree in Technical and Professional Communication with a specialization in Computer Science.

Return to Index - Add to Google - ics Calendar file

BTV - Saturday - 11:15-12:15 PDT

Title: Use opensource AI to map alerts & logs into techniques, clusters, and killchains
When: Saturday, Aug 10, 11:15 - 12:15 PDT
Where: LVCC West/Floor 3/W310 - Map

Description:

Introduction:
We will begin with an overview of event analysis systems and their challenges. Participants will learn about different types of data sources and logs, the prevalence of false positives, and the difficulty in identifying coordinated attacks. We will set the stage for the live, hands-on demonstration environment where participants can interact and apply what they learn in real-time. Importantly, no prior data science knowledge is required; all tasks will be performed using simple, user-friendly interfaces.

Introduction to MITRE ATT&CK Framework: An essential part of our session is understanding the MITRE ATT&CK framework. We will cover its structure, including Tactics, Techniques, and Procedures (TTPs), and explain why mapping alerts to this framework is crucial for standardizing threat detection and enhancing our capabilities.

Leveraging Open Source AI Tools: Next, we will delve into the open-source AI tools that will be used throughout the session. We will introduce families of algorithms including clustering and community detection, natural language processing with large language models (LLMs), and Markov chains. These tools are designed to be accessible and will be operated through straightforward interfaces. Participants will be guided through setting up a demo environment to follow along and interact with the exercises.

Data Preprocessing and Normalization: Participants will learn how to import and clean data from various sources, normalize data formats, and handle missing data. We will highlight some methods to get rich test data. This step is crucial for ensuring that the subsequent analysis is accurate and reliable. The hands-on exercise will involve preprocessing a sample dataset in real-time, using easy-to-follow steps and intuitive interfaces.

Mapping Alerts to MITRE ATT&CK Techniques: We will demonstrate techniques for mapping SIEM data to MITRE ATT&CK manually and using automated tools. The live demo will include a hands-on exercise where participants will map a sample dataset to MITRE ATT&CK Techniques, using AI to enhance mapping accuracy. All this will be done through simple interfaces that do not require deep technical knowledge.

Clustering Alerts into Contextualized Attack Steps: This section focuses on methods such as clustering and community detection. Participants will learn the criteria for clustering alerts based on temporal, spatial, and technical attributes. They will engage in a hands-on exercise to cluster sample alerts and evaluate the quality and relevance of the clusters, again using user-friendly interfaces.

Building Killchains: Participants will understand the concept and importance of killchains in cybersecurity. We will demonstrate methods for linking attack steps into a cohesive killchain, with a hands-on exercise to create a killchain from clustered data. Participants will analyze killchains to identify patterns and coordinated attacks, all through accessible interfaces.

Generating Actionable Tickets: We will outline the criteria for generating three types of tickets: FP Tickets, Incident Tickets, and Attack Story Tickets. Through a hands-on exercise, participants will generate sample tickets and learn how to ensure each ticket type is comprehensive and actionable. This process will be facilitated through simple interfaces that guide the user step-by-step.

Integrating and Automating the Workflow: Finally, we will discuss integrating this workflow into existing SOC setups and automating the process using scripts and tools. Participants will see how to maintain and update the system, ensuring continuous improvement in threat detection and response. The automation will be demonstrated in a way that requires minimal technical skills.

Q&A and Troubleshooting: The session will conclude with an open floor for questions, addressing common issues, and offering troubleshooting tips. Participants will also receive resources for further learning and support to continue enhancing their skills post-session.

Conclusion: By the end of this interactive session, participants will have hands-on experience using open-source AI tools to enhance their SOC capabilities. They will be able to map alerts to MITRE ATT&CK Techniques, cluster data into meaningful attack steps, and build comprehensive killchains to uncover coordinated attacks. Additionally, they will learn to generate actionable tickets to facilitate immediate response and long-term improvements in their security posture. All of this will be achieved without needing advanced data science knowledge, thanks to the simple and intuitive interfaces provided.

Participants are encouraged to apply these techniques in their own environments and continue exploring the vast capabilities of open-source AI in cybersecurity. The live demo environment setup will provide a practical and engaging way to solidify these concepts and skills.

Given a SIEM loaded with alerts, logs and events from a variety of data sources, your task is to find the coordinated attack in the LOTS of noise of false positives & lone incidents.

Together we will use opensource AI tools to map all of the hetrogenous data on the SIEM to MITRE ATT&CK Techniques, and then Cluster based on a variety of attributes to form contetualized Attack Steps. We will then fuse these attack steps based on timeline, causality and assets involved into killchains to reveal coordinated attacks.

You are required to output the following tickets: 1. FP Ticket that has clusters of false positives and tuning advisories & suggestions that should be forwarded to detection engineering to tune.

1. Incident Ticket that has remediation & investigation advisories & action playbooks for the contextualized lone-incidents identified.
2. Attack Story Ticket that has a correalted set of clusters of alerts & logs revealing a coordinated attack killchain affecting a variety of assets over a stretch of time.

SpeakerBio: Ezz Tahoun

Ezz Tahoun, a distinguished cyber-security data scientist, who won AI & innovation awards at Yale, Princeton and Northwestern. He also got innovation awards from Canada's Communications Security Establishment, Microsoft US, Trustwave US, PIA US, NATO, and more. He ran data science innovation programs and projects for OrangeCyber Defense, Forescout Technologies, Royal bank of Canada, Governments, and Huawei Technologies US. He has published 20 papers, countless articles and 15 open source projects in the domain. When he was 19 years old he started his CS PhD in one of the top 5 labs in the world for cyber & AI, in the prestigious University of Waterloo, where he published numerous papers and became a reviewer for top conferences. His designations include: SANS/GIAC-Advisory-Board, aCCISO, CISM, CRISC, GCIH, GFACT, GSEC, CEH, GCP-Professional-Cloud-Architect, PMP, BENG and MMATH. He was an adjunct professor of cyber defense and warfare at Toronto's school of management.

Return to Index - Add to Google - ics Calendar file

PYV - Friday - 11:30-12:40 PDT

Title: User Behaviour Analytics in Payments
When: Friday, Aug 9, 11:30 - 12:40 PDT
Where: LVCC West/Floor 2/W202 - Map

Description:

User Behaviour Analytics are powerful predictors of both genuine and anomalous behaviour in payments. This talk will work through a few examples of payment fraud scenarios and is aimed at demonstrating the thought processes of computing effective indicators of fraud. This talk should be of interest to people interested in payments but also analysts using UEBA systems in cybersecurity.

SpeakerBio: Karthik Tadinada, Founder at Fortify Solutions

Karthik Tadinada is the founder of Fortify Solutions, a payment risk prevention company. Karthik has built high performing fraud prevention models for credit and debit card payments, account-to-account transfers, e-commerce merchants and national payment rails. Models he and his teams built score all the debit card transactions in Australia, a double digit percentage of the credit card transactions in the US and the majority of Point of Sale transactions in the UK.

Return to Index - Add to Google - ics Calendar file

PHV - Saturday - 10:00-10:59 PDT

Title: Using AI Computer Vision in Your OSINT Data Analysis
When: Saturday, Aug 10, 10:00 - 10:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

OSINT is a great mechanism for the collection of data, but what do you do with all of it once it's collected? It can take significant time with the human eye to analyze each image or video. Furthermore, you may miss important artifacts in the foreground or background. Computer vision can churn through the plethora of data to pull out the relevant evidence at lightning speed. For the last 5 years we've been exploring the use of Azure and AWS for computer vision to rapidly process large sets of image and video data acquisitions for forensic evidence.Through the use of AI we have analyzed thousands of images and videos to perform object detection, facial recognition, OCR, voice to text analysis, and more. In this session we'll explore the use of cloud platforms to exponentially increase your analysis of uncovering key artifacts to your case using demos and real world examples. We then apply chronolocation analysis to allow an investigator to paint a true-life narrative, for example an individual with a weapon at a location at a particular time. We'll provide live demos of common scenarios to reveal benefits to processing your data collections in a rapid, efficient, comprehensive, and accurate manner. We'll then wrap-up the presentation with additional AI computer vision recommendations and resources.

SpeakerBio: Mike Raggo

Michael T. Raggo has over 30 years of security research experience. During this time, he has uncovered and ethically disclosed vulnerabilities in products including Samsung, Checkpoint, and Netgear. Michael is the author of "Mobile Data Loss: Threats & Countermeasures" and "Data Hiding" for Syngress Book. He is also a frequent presenter at security conferences, including Black Hat, DEF CON, Gartner, RSA, DoD Cyber Crime, OWASP, SANS. He was also awarded the Pentagon's Certificate of Appreciation.

Return to Index - Add to Google - ics Calendar file

ICSV - Friday - 10:00-10:50 PDT

Title: Using ChatGPT to Write Defensive & Offensive Tools for ICS/OT
When: Friday, Aug 9, 10:00 - 10:50 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

During the work on my SANS Master's thesis, I realized two things: I am not a developer and ChatGPT makes a pretty good one. Using ChatGPT to write the Python scripts for my research, I started to branch out and use it to write defensive tools such as for identifying unknown assets on the network as a listening service or offensively such as when taking a PLC out of Run mode remotely. If you can think through the process, ChatGPT (or other GenAI) can help you make it a reality. Want to Live off the Land and don't want to download a Python script which might be spotted? Use ChatGPT to convert it to PowerShell on the spot! Receiving error messages from the code it wrote for you? Don't worry - it can fix those issues too! The presentation will walk attendees through prompt creation for two sample coding projects - both with offensive/defensive capabilities, tools that attendees would be able to use back on the job. And, with inspiration, go out and create their own tools!

SpeakerBio: Mike Holcomb, Fellow of Cybersecurity and ICS/OT Cybersecurity Global Lead at Fluor

Mike helps people learn how to secure Industrial Control Systems (ICS)/Operational Technology (OT) environments, from engineers and IT cyber security team members to asset owners and operators. He is the Fellow of Cybersecurity and the ICS/OT Cybersecurity Global Lead for Fluor, one of the world's largest engineering, procurement, and construction companies. His current role provides him with the opportunity to work in securing some of the world's largest ICS/OT environments, from power plants and commuter rail to manufacturing facilities and refineries. He has his Masters degree in ICS/OT cybersecurity from the SANS Technology Institute. Additionally, he maintains more than a few cyber security and ICS/OT certifications.

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 12:30-12:59 PDT

Title: Using EPSS for Better Vulnerability Management
When: Sunday, Aug 11, 12:30 - 12:59 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

The Exploit Prediction Scoring System (EPSS) provides efficient, data-driven vulnerability management data that uses current threat information from CVE and real-world exploit that helps understand the probability that a vulnerability will be exploited.

This talk will discuss the EPSS model in-depth and demonstrate how to implement EPSS for CI/CD pipelines and more traditional operating systems and application patching.

SpeakerBio: jgamblin

Researcher. Builder. Hacker. Traveler.

Return to Index - Add to Google - ics Calendar file

RTV - Saturday - 15:00-15:50 PDT

Title: Using Retrieval Augmented Generation (RAG), Langchain, and LLMs for Cybersecurity Operations
When: Saturday, Aug 10, 15:00 - 15:50 PDT
Where: LVCC West/Floor 2/W204-W207/W204-W207-Narrows - Map

Description:

Everyone is trying to leverage AI for many tasks. However, are they doing it effectively? This presentation explores the integration of Retrieval Augmented Generation (RAG), Langchain, and Large Language Models (LLMs) within cybersecurity and offensive security operations. We will begin by exploring the conceptual foundations of these technologies, looking at their unique capabilities for enhancing automation in offensive (and defensive) security operations.

We will go over different practical demonstrations and case studies. You will gain insights into how these tools can be harnessed to take your red, blue, purple team to the next level. We will discuss the implementation of RAG for dynamic information retrieval, re-ranking, and other techniques and how Langchain is making using these technologies so easy nowadays. We will also explore the use of uncensored models that can be used for cybersecurity and to create exploits.

SpeakerBio: Omar Santos
No BIO available

Return to Index - Add to Google - ics Calendar file

CHV - Friday - 13:00-13:30 PDT

Title: V2GEvil: Ghost in the wires
When: Friday, Aug 9, 13:00 - 13:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

This research aims to enhance electric vehicle cybersecurity by uncovering vulnerabilities in the Electric Vehicle Communication Controller (EVCC), crucial for charging communication. We've developed a specialized security tool after examining electric vehicle charging ports and On-Board Charging (OBC) protocols, with a focus on ISO 15118 standards.

Speakers: Pavel Khunt,Thomas "Cr0wTom" Sermpinis

SpeakerBio: Pavel Khunt, Automotive Security Researcher and Penetration Tester at Auxilium Pentest Labs

Pavel Khunt is an Automotive Security Researcher and Penetration Tester at Auxilium Pentest Labs. With a background in engineering, Pavel graduated from FIT CTU, where his master's thesis focused on V2G (Vehicle-to-Grid) communication during the charging of Electric Vehicles (EVs). Passionate about ensuring the safety and security of automotive technologies.

SpeakerBio: Thomas "Cr0wTom" Sermpinis, Technical Director at Auxilium Pentest Labs

Thomas Sermpinis (a.k.a. Cr0wTom) is the Technical Director of Auxilium Pentest Labs and independent security researcher with main topics of interest in the automotive, industrial control, embedded device, and cryptography sectors. During his research, he published several academic papers, 0days and tools with the ultimate goal of making the world a safer place, but also helped almost 200 OEMs and Tier 1 automotive suppliers to achieve better security and develop more secure products.

Additionally, he spoke in several highly technical security conferences, presenting his research and trying to create safer streets for drivers, passengers, pedestrians, and everyone in the street, including Zer0Con, TyphoonCon, TROOPERS, DeepSec and others.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 12:00-13:15 PDT

Title: Veilid Dev and Community Meetup
When: Friday, Aug 9, 12:00 - 13:15 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:
SpeakerBio: The_Gibson
No BIO available

Return to Index - Add to Google - ics Calendar file

SOC - Friday - 12:00-13:30 PDT

Title: Veilid Dev and Community Meetup
When: Friday, Aug 9, 12:00 - 13:30 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

Cult of the Dead Cow and Hackers.Town are bringing you a meet and greet and chat session about Veilid Framework. Come by, say hi, talk shop, let’s see each other in person and have a little fun! Veilid Foundation directors and many of the primary contributors will be there to share progress over the last year. Come by and help us to restore the future and ensure the privacy of the internet for generations to come!

Return to Index - Add to Google - ics Calendar file

CON - Sunday - 10:00-12:59 PDT

Title: venator aurum - A Treasure Hunt
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: Other / See Description

Description:

Travel the seven seas to the seven wonders across time to test your skills across both old and new worlds. Every journey's end yields its own reward, but there is only one who can claim to be the first to the summit. Bring your entire tech arsenal or just a phone. Start at the broken compass and push forward into the known to seek the unknown. Wonders, plunder, and glory to those who test the waters and themselves.

Return to Index - Add to Google - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: venator aurum - A Treasure Hunt
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: Other / See Description

Description:

Travel the seven seas to the seven wonders across time to test your skills across both old and new worlds. Every journey's end yields its own reward, but there is only one who can claim to be the first to the summit. Bring your entire tech arsenal or just a phone. Start at the broken compass and push forward into the known to seek the unknown. Wonders, plunder, and glory to those who test the waters and themselves.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: venator aurum - A Treasure Hunt
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: Other / See Description

Description:

Travel the seven seas to the seven wonders across time to test your skills across both old and new worlds. Every journey's end yields its own reward, but there is only one who can claim to be the first to the summit. Bring your entire tech arsenal or just a phone. Start at the broken compass and push forward into the known to seek the unknown. Wonders, plunder, and glory to those who test the waters and themselves.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: Vendors and Exhibitors Open
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West - Map

Description:

This is when you can go visit our awesome vendors.

We don't know which they will be accepting cash vs cards. That's up to each organization, and we do not have a list.

We also don't know if/when vendors will sell out of anything they may be selling.

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: Vendors and Exhibitors Open
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West - Map

Description:

This is when you can go visit our awesome vendors.

We don't know which they will be accepting cash vs cards. That's up to each organization, and we do not have a list.

We also don't know if/when vendors will sell out of anything they may be selling.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: Vendors and Exhibitors Open
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West - Map

Description:

This is when you can go visit our awesome vendors.

We don't know which they will be accepting cash vs cards. That's up to each organization, and we do not have a list.

We also don't know if/when vendors will sell out of anything they may be selling.

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 21:00-01:59 PDT

Title: VETCON
When: Saturday, Aug 10, 21:00 - 01:59 PDT
Where: LVCC West/Floor 1/W106-W109-Chillout 1 - Map

Description:

Welcome to VETCON, the DEFCON Community event and of course, THE VETCON Party where veterans, active duty military, and even civilians looking for a taste of the action come together for a cyber rendezvous. Because let's face it, sometimes you need a little civilian perspective to hack the system!

Return to Index - Add to Google - ics Calendar file

ADV - Sunday - 12:00-12:59 PDT

Title: Village closing
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 4/HW4-03-05/ADV stage - Map

Description:

Village closing ceremony

SpeakerBio: Adversary Village Crew
No BIO available

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 13:00-13:59 PDT

Title: Virtual SIEM/SOAR Workshop
When: Saturday, Aug 10, 13:00 - 13:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

What exactly are SIEM and SOAR and why are they so critical to the cyber securitylandscape? In today's session, I want to explore the ins and outs of SIEM and SOAR platforms and how they can be scaled up and down from smaller businesses all the way to multiple billion-dollar firms and their security organizations. I will also be covering how learning and understanding automation and having soft skills in this space can set you apart from the competition and help you land a role faster. Anyone who is interested in the blue side of cybersecurity doesn't want to miss this.

SpeakerBio: Kenneth Ellington, Senior Cybersecurity Consultant

Kenneth Ellington is rising cybersecurity professional who is dedicated to nurturing new cybersecurity talent. A Florida native now based in Dallas-Fort Worth Texas, he’s leveraged his unyielding drive to go from working at the deli counter to landing a Big 4 Senior Cybersecurity Consulting role - all within 3 fast-paced years. His current specialties are in SIEM, SOAR, and endpoint security.

In his trainings, Kenneth brings that same energy and passion to students as they learn about security solutions and address real-world scenarios. He also used to teach Cyber Infrastructure part-time at the University of Houston, volunteers for the non-profit Blacks in Cyber Security (BIC), and trains in boxing and kickboxing in his free time.

Return to Index - Add to Google - ics Calendar file

AIxCC - Saturday - 17:15-17:59 PDT

Title: Visualizing AIxCC: Bringing Your Code to Life
When: Saturday, Aug 10, 17:15 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-06/HW3-05-06-Stage - Map

Description:

There are few opportunities to learn how code can be transformed into a visualization project. Tune in as Mark Griffin from UnDaunted shares about how his team took the competitor submissions and translated them into the AIxCC competition experience at DEF CON.

SpeakerBio: Mark Griffin, Undaunted

I'm an developer, hacker, and software explainer.

After writing/reading software and finding bugs in code professionally for over a decade, I became fascinated by how people understand and interact with code… so I've made it my mission to help people see and understand code better.

I started my career in a variety of cyber security roles: doing network traffic analysis, analyzing code security, reverse-engineering malware, etc. Along the way I've been lucky to have worked with truly awesome people on cool projects, and have done a bunch of amazing and random things like:

- Spoke at ShmooCon and several smaller conferences
- Wrote code for a variety of projects in areas like custom debugging, security, fuzzing, and RE (such as bncov and Ariadne)
- Served as adjunct faculty, instructor, and trainer in several roles, including teaching an undergrad course
- Found some bugs in well known-software (some public CVEs, but mostly private engagements on software ranging from embedded systems to decentralized finance)
- Played in numerous Capture-the-Flag (CTF) computer security competitions, and helped organize a couple (such as LiveCTF)

Return to Index - Add to Google - ics Calendar file

DL - Friday - 10:00-11:45 PDT

Title: Volatile Vault - Data Exfiltration in 2024
When: Friday, Aug 9, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W305 - Map

Description:

In red team operations, selecting the right tools for data exfiltration is critical, yet comes with obstacles such as triggering Data Exfiltration Prevention (DEP) systems. We present "Volatile Vault" as a solution, a custom-built platform tailored to evade DEP detection. Our tool encrypts the data on the client-side and then provides a modular approach for uploading said data. Some of the currently implemented upload strategies are chunked HTTP uploads to multiple domain fronted endpoints (AWS) or QUIC as an alternative protocol.

Speakers: Moritz Laurin Thomas,Patrick Eisenschmidt

SpeakerBio: Moritz Laurin Thomas, Senior Red Team Security Consultant at NVISO ARES

Moritz is a senior red team security consultant at NVISO ARES (Adversarial Risk Emulation & Simulation). He focuses on research & development in red teaming to support, enhance and extend the team’s capabilities in red team engagements of all sorts. Before joining the offensive security community, Moritz worked on a voluntary basis as a technical malware analyst for a well-known internet forum with focus on evading detections and building custom exploits. When he isn’t infiltrating networks or exfiltrating data, he is usually knees deep in research and development, dissecting binaries and developing new tools.

SpeakerBio: Patrick Eisenschmidt, Red Team Lead at NVISO ARES

Patrick has gained extensive experience in the offensive security domain. Currently, he serves as the Red Team Lead at NVISO ARES (Adversarial Risk Emulation & Simulation). In this role, he supervises a team of operators and directs both high-profile Red Team operations and Tiber/TLPT Assessments. Beyond leadership, Patrick actively participates in crafting intricate spear phishing campaigns and boosts the Red Team's effectiveness by developing and maintaining open-source methodologies and tools.

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 10:00-10:45 PDT

Title: Voting Village Opening Remarks
When: Saturday, Aug 10, 10:00 - 10:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:
Speakers: Catherine Terranova,Harri Hursti,Matt Blaze

SpeakerBio: Catherine Terranova

Catherine Terranova is a Columbia University alumna and researcher. Her current focus is on cyber security and election integrity with an emphasis on misinformation, disinformation, and malinformation, known as information integrity. Ms. Terranova joined the team in 2021 and has been growing and developing the Voting Village since DEF CON 29. She heads all aspects of the program and manages other related projects focused on the global preservation of democracy.

SpeakerBio: Harri Hursti
No BIO available
SpeakerBio: Matt Blaze

Matt Blaze is one of the original co-founders of the Voting Village and is currently the McDevitt Professor of Computer Science and Law at Georgetown University. He has over two decades of experience with election system security, and his current research focuses on security, privacy, and robustness in large scale systems with an emphasis on problems at the intersection of technology and public policy.

Return to Index - Add to Google - ics Calendar file

DL - Saturday - 14:00-15:45 PDT

Title: Vovk - Advanced YARA Rule Generator v2.0
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W304 - Map

Description:

Vovk is a toolset that can be used to create YARA rules. The Vovk DEF CON 2024 version will be released at DEF CON.

Speakers: Benjamyn Whiteman,Vishal Thakur

SpeakerBio: Benjamyn Whiteman, Lead Analyst, Global CSOC at TikTok USDS

Benjamyn Whiteman has worked in the InfoSec industry for the past 7 years in roles that include Security Engineering, Forensics Analysis and Global CSIRTs. Ben regularly presents his research at internal company summits and security conferences. Ben has been training and mentoring new cyber security professionals for a few years now and also presented his research at HackSydney 2022 and 2023. Currently, Ben is a part of the Global CSOC for TikTok USDS as the Lead Analyst at Sydney, Australia.

SpeakerBio: Vishal Thakur, Senior Director, Cyber Fusion Center at TikTok USDS

Vishal Thakur has worked in the information security industry for many years in hands-on technical roles, specializing in Incident Response with a heavy focus on Emerging Threats, Malware Analysis and Research. He has presented his research at international conferences (BlackHat, DEFCON, FIRST, SANS DFIR Summit) and has also run training/workshops at some of these conferences. Vishal is currently working as Senior Director, Cyber Fusion Center at TikTok USDS. In past roles, Vishal worked as a Senior Researcher at Salesforce, helping their Incident Response Centre with advanced threat analysis and developing DFIR tools and has been a part of the Incident Response team at the Commonwealth Bank of Australia. For the past few years, Vishal has been involved in ML and AI security and has been researching this subject.

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 15:00-15:30 PDT

Title: War Games: Red Team for OT (Based on Real World Case Studies)
When: Saturday, Aug 10, 15:00 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

In this talk, Shishir will share some critical insights from performing a decade worth of Red Team (attack simulation) exercises for large-scale industrial operations across the globe.

The presentation will also cover real-world examples of attack vectors leveraged by Google's Mandiant Red Team while performing offensive security exercises for operational technology and control system environments.

This talk will cover:

- Insights into common TTPs and attack vectors for large-scale industrial networks
- Network propagation and mission execution across ICS-OT attack life-cycle
- Examples from real-world case studies of penetrating cyber-physical systems

SpeakerBio: Shishir Gupta, Technical Manager and Function Lead, ICS-OT Red Team at Mandiant

Shishir specialises in offensive security for critical infrastructure and operational technology, and has led penetration testing and attack simulation (red team) exercises for 50+ industrial operations across the globe. He has a unique experience of conducting technical assessments across a wide variety of critical infrastructure and cyber physical sectors (including power and utilities, road transportation, rail transportation, air traffic control, industrial manufacturing, resource mining, oil and gas, telecommunications and building management systems). In his current role, Shishir serves as Technical Manager and Function Lead for ICS-OT Red Team at Mandiant (a Google company).

Return to Index - Add to Google - ics Calendar file

SOC - Sunday - 10:30-12:20 PDT

Title: WarDriver Meetup
When: Sunday, Aug 11, 10:30 - 12:20 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 11:30-11:59 PDT

Title: Warflying in a Cessna
When: Sunday, Aug 11, 11:30 - 11:59 PDT
Where: LVCC West/Floor 1/Hall 3/Creator Stage 2 - Map

Description:

Wardriving is cool, and airplanes are cool. What happens if we combine the two? Is it safe? Is it legal? How much WiFi is it possible to see from an airplane? How far does WiFi leak into the atmosphere? How far away can we see an access point? Can we catch a specific network at 1500 feet above the ground? How about 2500? We loaded up a small plane and flew around in circles to find out. This talk will share both our preparation and our results, including figuring out the best places to warfly, what equipment to use, and how to do it safely. We will present the flights we made, the data we gathered, how we analyzed it, and what we discovered. (Spoiler alert: flying a Cessna is a really, really non-stealthy way to collect information about wireless access points.)

Speakers: Matt Thomassen,Sean McKeever

SpeakerBio: Matt Thomassen, Security Architect at a financial organization

Matthew Thomassen has been doing computer security since before it was cool and is currently a Security Architect in a financial organization, with previous experience in the consumer healthcare and automotive sectors, which afforded him the opportunity to help with random things in the early days of the Car Hacking Village. He is a certified Commercial Pilot with Multiengine and Instrument ratings, as well as an Airframe & Powerplant Mechanic. He is also an Extra Class Amateur Radio operator and has an MBA, though he tries not to live and die by Excel spreadsheets.

SpeakerBio: Sean McKeever, Senior Security Researcher at GRIMM

Sean McKeever is a Senior Security Researcher at GRIMM, specializing in automotive/mobility security, and embedded systems reverse engineering. Previously he worked as a Cybersecurity Architect at global automotive OEM where he secured advanced transportation mobility platforms and served as the company's Bug Bounty Program Manager. Outside of Sean's employment, he co-founded the Detroit chapter of the Automotive Security Research Group (ASRG), developed the RoboCar Platform, and has contributed to Car Hacking Village CTFs for DEFCON and GRRCon, and the general CTFs for Converge and BSides Detroit.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 15:30-15:55 PDT

Title: Warwheeling: The Wireless Sk8r
When: Friday, Aug 9, 15:30 - 15:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

Welcome to the next generation of wardriving, where we encourage you to step outside, breathe in the fresh air, and shred the streets as you're collecting ALL the WIFI. In this presentation, we'll dive into the world of Warwheeling, a novel twist on wardriving that involves using a onewheel or any PEV as your mobile exploration hub.

SpeakerBio: r1otctrl, SOCC Analyst

Hi! I'm Riøt, a SOCC analyst by day and a warwheeler by night.

I'm active in hacker circles like the #Wardriving group on WiGLE, DCG561/305, and Boca 2600. My Onewheel community includes SoFlow, Float Gang, and Orlando Onewheel.

My favorite way to touch grass is by going on long Onewheel rides. It's a great opportunity to stress-test new rigs while out in the wild.

I'm still new to RF, but the past year has been a valuable learning experience in optimizing wireless capture while staying lightweight. Through posting warwheeling content on Instagram, I've connected with others who also found an interest in wardriving while also choosing a PEV as their mode of transport.

Return to Index - Add to Google - ics Calendar file

ASV - Sunday - 11:00-12:59 PDT

Title: Watch The Skies: Build Your Own ADS-B receiver
When: Sunday, Aug 11, 11:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-07-02/HW2-07-02-Workshops - Map

Description:

In this workshop we will build an inexpensive ADS-B (Automatic Dependent Surveillance–Broadcast) receiver with a Raspberry Pi and RTL-SDR. The receiver will track and display aircraft (commercial, private, and military) providing real-time altitude, direction, speed, GPS location and aircraft information. We'll discuss ADS-B technology and its importance to air traffic control. We'll also discuss building cheap external antennas to improve reception.

We will have 10 FREE ADS-B receiver kits that will be given away, at our discretion, to middle through high school students (11-18 years old). An additional 10 ADS-B kits will be available to any attendee for a modest donation to the Aerospace Village. Please see the Aerospace Village control tower to reserve your spot.

SpeakerBio: Jim "Gurney" Ross

Jim "Gurney" Ross is an aerospace cybersecurity engineer with over 30 years of experience in aerospace systems (commercial and defense) and over 20 years of experience in cybersecurity. He is a co-founder of the Aerospace Village and a longtime DEFCON attendee. Gurney has built and operated an ADS-B receiver at the Aerospace Village for the past five years displaying. live, local LAS aircraft data. He is the youth and STEM point of contact for the Aerospace Village.

Return to Index - Add to Google - ics Calendar file

DC - Saturday - 16:30-17:15 PDT

Title: Watchers being watched: Exploiting the Surveillance System and its supply chain
When: Saturday, Aug 10, 16:30 - 17:15 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:

With the development of artificial intelligence and image processing technology, the video industry such as CCTV is developing greatly. However, CCTV video may infringe on an individual's privacy, and personal information may be leaked due to hacking or illegal video collection. As such, Surveillance System's Security issues are also increasing, the importance of the video surveillance industry is becoming more prominent.

In order to prevent hacking or illegal video collection, research on camera security is being conducted. However, there is a lack of awareness of NVR (Network Video Recorder), a device that actually watches videos recorded by cameras, and research on this is also insufficient.

We selected Hikvision and Dahua, which have a high NVR market share, as target vendors, and also selected Synology's NVR-related package, Surveillance Station, as targets. Before proceeding with vulnerability analysis, several problems occurred during the file system extraction process, but U-Boot mitigation was successfully bypassed through various methods. Afterwards, various types of vulnerabilities were discovered through analysis, and OEM verification was also conducted to increase impact. We present exploit scenarios for surveillance devices through vulnerability linkage and present supply chain security issues in the Surveillance System.

1. link
2. link
3. link
4. link
5. link
6. link
7. link
8. link
9. link
10. link
11. link
12. link
13. link
14. link
15. link
16. link

Speakers: Chanin Kim,Myeonghun Pak,Myeongjin Shin

SpeakerBio: Chanin Kim, Offensive Researcher at S2W Inc

Chanin Kim has previously conducted offensive research and has experience discovering vulnerabilities in various places, including Windows, Rust, and OpenVPN. Chan In-Kim is also currently working as an Offensive Researcher at S2W Inc in Korea and is conducting various offensive research.

SpeakerBio: Myeonghun Pak, Researcher at KITRI

Myeonghun Pak is currently a university student and is working on offensive research. He enjoys analyzing embedded vulnerabilities.

SpeakerBio: Myeongjin Shin, Student at Chonnam National University

Myeongjin Shin is currently a student at Chonnam National University and belong to SRC lab. He is interested in vulnerability analysis and research.

Return to Index - Add to Google - ics Calendar file

BICV - Saturday - 12:15-12:59 PDT

Title: Weaponized Convenience: Inside the Rise of Remote Tool Abuse
When: Saturday, Aug 10, 12:15 - 12:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

In an era of remote work and distributed IT environments, remote administration tools (RATs) and remote monitoring and management (RMM) tools have become indispensable for system administrators and managed service providers (MSPs). However, the same features that make these tools efficient also make them attractive targets for malicious actors. Advanced threat actors are increasingly leveraging legitimate RATs and RMMs to gain unauthorized access to networks, bypassing traditional security controls and evading detection.

Speakers: Nader Zaveri,Fernando Tomlinson

SpeakerBio: Nader Zaveri, Incident Response & Remediation Senior Manager

Nader Zaveri has over 15 years in the cybersecurity industry, and holds over a dozen industry-related certifications as well as an author and a regular speaker at industry events. Specializing in incident response and remediation, particularly against complex threats like nation-states and ransomware, he has also led post-incident transformational projects in security and infrastructure. Nader's experience spans leadership roles in top cybersecurity firms and multinational organizations. Apart from his professional pursuits, he mentors young professionals and has served on the boards of various startups, contributing significantly to their growth and success.

SpeakerBio: Fernando Tomlinson, Forensics and Incident Response Technical Manager at Mandiant / Google Cloud

Fernando Tomlinson is a Technical Manager for Digital Forensics and Incident Response at Mandiant/ Google Cloud. Prior to that, he served in the U.S. Army where he retired as a Cyber Warrant Officer. While serving, he was the Senior Technical Advisor for forensics and malware analysis at the U.S. Army Cyber Command, responsible for the defensive actions of all U.S. Army systems. He also served as a Technical Director of a Cyber Operations Center and has led multi-level Digital Forensics and Incident Response and threat hunting teams. Additionally, he is an Adjunct Professor at the University of Arizona and enjoys contributing to the community.

Return to Index - Add to Google - ics Calendar file

APV - Saturday - 14:00-14:30 PDT

Title: Web2 Meets Web3: Hacking Decentralized Applications
When: Saturday, Aug 10, 14:00 - 14:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Dapps (decentralized applications) are a type of application in the blockchain space that integrate both Web2 and blockchain components, presenting unique security challenges. Drawing from years of experience hacking Dapps, this session will share real-world examples of Dapp vulnerabilities and attack vectors. Topics covered include an introduction to Dapps, Dapp threat modeling, and Dapp vulnerability case studies, providing valuable insights and resources for newcomers and seasoned Web2 pentesters looking to enhance their Web3 application hacking skills.

SpeakerBio: Peiyu Wang

Peiyu is a Security Engineer at CertiK, a blockchain security company, where he has the chance to hack various blockchain products. Outside of work, he enjoys aping into meme coins, trading, and playing video games.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-10:59 PDT

Title: Welcome / Badge & Swag Pick Up
When: Friday, Aug 9, 10:00 - 10:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-03 - Map

Description:

Pick up your DCNextGen badge and other swag. We will also have an overview of DCNextGen activities and adventures!

Return to Index - Add to Google - ics Calendar file

DC - Friday - 10:00-10:20 PDT

Title: Welcome to DEF CON
When: Friday, Aug 9, 10:00 - 10:20 PDT
Where: LVCC West/Floor 1/Hall 1/Track 1 - Map

Description:
SpeakerBio: Jeff "The Dark Tangent" Moss, DEF CON Communications
No BIO available

Return to Index - Add to Google - ics Calendar file

VMV - Saturday - 16:30-16:59 PDT

Title: What Do Long Voter Registration Lines Mean?
When: Saturday, Aug 10, 16:30 - 16:59 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

We often hear about long lines at polling places and in particular at voter registration sites. Unfortunately, we rarely get insight into why this is happening and why this happens in such specific geographic locations. Join us to hear the full breakdown of what is happening from one of the Voting Village original founders and former White House Principal Deputy National Cyber Director and premier voting expert.

SpeakerBio: Jake Braun

Jake Braun was appointed by President Joseph Biden as Senior Advisor to the Department of Homeland Security in February of 2021 where he focuses on Management issues. He is also a lecturer at the University of Chicago Harris School of Public Policy. He works at the center of politics, technology and national security to advance the field of cyber policy. He is the author of Democracy in Danger: How Hackers and Activists Exposed Fatal Flaws in the Election System and has co-authored two award-winning and seminal works on election infrastructure cyber vulnerabilities. Mr. Braun has worked extensively on national security and finance issues throughout the U.S., Europe, Asia, Africa, Middle East and Latin America. Prior to joining the University of Chicago Harris School of Public Policy faculty and Cambridge Global Advisers, Mr. Braun was appointed by President Obama as White House Liaison to the Department of Homeland Security (DHS) where he oversaw some of the most high profile public engagements executed at DHS. He was instrumental in the effort to gain passage in the European Parliament of the largest big data sharing agreement in history between the United States and the European Union. In addition, he designed and implemented a program to modernize the DHS cybersecurity workforce. Mr. Braun also oversaw stakeholder crisis communications for the White House during the 2010 Deep Water Horizon Gulf Oil Spill.Prior to his tenure as White House Liaison, Mr. Braun served on the Presidential Transition Team for the Obama Administration as Deputy Director for the National Security Agencies Review. In this capacity he oversaw agency review programs for all national security agencies including the State Department, DOD, DHS, CIA, USAID, etc. and guided policy assessments from their inception to the President-Elect's desk. Mr. Braun also designs and implements political campaigns in the U.S., Asia, Africa, Latin America and Europe. Before coming to Washington, Mr. Braun served as the National Deputy Field Director to the 2008 Obama for America Campaign, overseeing an effort that utilized the most sophisticated grassroots, social media and data analysis available.In addition to his role at Harris, Mr. Braun is co-founder of the DEF CON Voting Machine Hacking Village, in the President's Circle on the Chicago Council on Global Affairs, and a strategic advisor to the Department of Homeland Security and the Pentagon on cybersecurity. DEF CON is the largest hacker conference in the world and in cooperation with them he has co-authored two fundamental and critically acclaimed reports on election infrastructure cyber vulnerabilities, The DEF CON 25 and 26 Voting Village Reports.

Return to Index - Add to Google - ics Calendar file

VMV - Friday - 14:45-15:30 PDT

Title: What Does it Mean to be an American?
When: Friday, Aug 9, 14:45 - 15:30 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

What does it mean to be an American? Or perhaps what should it mean? The world we live is now more complex then ever, with technology, law, policy, threats to personal wellbeing and international conflict dominating the headlines, how do Americans manage to stay in engaged in the affairs that control their society? This talk will be structured as a short presentation leading to an open forum discussion positioned to discover what it means to be an American in this current climate. We'll discuss civics, generational gaps, and the role of technology in addressing the active citizen today. We're all here to defend and support democracy, but that starts with a conversation.

SpeakerBio: Kendall Spencer

Kendall Spencer wears a variety of interesting hats on a day to day basis. As a professional athlete, he's represented the United States in competition globally. But he is also the first black antique and rare book dealer in the US. Specializing in American history, he uses his experiences in the book trade to address how we might learn from history and restore democracy. Currently he is a lawyer at Ropes & Gray LLP, where he specializes in technology, cybersecurity, and corporate transactions.

Return to Index - Add to Google - ics Calendar file

VMV - Friday - 10:00-10:45 PDT

Title: What is the Voting Village?
When: Friday, Aug 9, 10:00 - 10:45 PDT
Where: LVCC West/Floor 2/W223-W224 - Map

Description:

Brief overview of what the Voting Village is, it's mission, it's goals, and it's history.

Speakers: Catherine Terranova,Matt Blaze,Harri Hursti

SpeakerBio: Catherine Terranova

Catherine Terranova is a Columbia University alumna and researcher. Her current focus is on cyber security and election integrity with an emphasis on misinformation, disinformation, and malinformation, known as information integrity. Ms. Terranova joined the team in 2021 and has been growing and developing the Voting Village since DEF CON 29. She heads all aspects of the program and manages other related projects focused on the global preservation of democracy.

SpeakerBio: Matt Blaze

Matt Blaze is one of the original co-founders of the Voting Village and is currently the McDevitt Professor of Computer Science and Law at Georgetown University. He has over two decades of experience with election system security, and his current research focuses on security, privacy, and robustness in large scale systems with an emphasis on problems at the intersection of technology and public policy.

SpeakerBio: Harri Hursti
No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 11:15-11:59 PDT

Title: What To Expect When You're Exploiting: Attacking and Discovering Zero-Days in Baby Monitors and Wi-Fi Cameras

When: Saturday, Aug 10, 11:15 - 11:59 PDT

Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Home surveillance technology is a modern convenience that has been made accessible to the masses through the rise of IoT devices, namely cloud-connected Wi-Fi cameras. From parents monitoring their infants to homeowners watching their entryways, these cameras provide users with access to instant, high definition video from the convenience of a mobile phone, tablet, or PC. However, the affordability of these devices and relative ease of cloud access generally correlates to flawed security, putting users at risk. We set out to explore the attack surface of various Wi-Fi camera models to gain a deeper understanding of how these devices are being exploited. In the end, we devised methods to gain local root access, uncovered user privacy issues, discovered a zero-day vulnerability within a prominent IoT device management platform that allows attackers to gain remote control of millions of cameras worldwide and access sensitive user data, and revealed how these devices may be vulnerable to remote code execution attacks through completely unauthenticated means thanks to an inherently flawed implementation of their underlying peer to peer networking protocol. Along with demonstrating our exploits against live cameras, we will highlight the methods used to obtain our most significant findings and provide guidance on remediating the issues we encountered so these devices can be used safely in your household. We will also invite audience members to probe and attack a camera during our talk and earn a prize in the process!

Speakers: Eric Forte,Mark Mager

SpeakerBio: Eric Forte, Security Research Engineer at Elastic

Eric Forte is a Security Research Engineer at Elastic with a background in embedded systems and streaming data analysis. He has worked in technical leadership roles in engineering Low Size Weight and Power (SWaP) capabilities and network security solutions. As part of this work, he managed an IoT research and reverse engineering lab to help in the development of these different capabilities for various organizations across the United States.

SpeakerBio: Mark Mager, Lead, Endpoint Protections Team at Elastic

Mark Mager leads the Endpoint Protections Team at Elastic. He has served in prominent technical leadership roles in the research and development of advanced computer network operations tools and has provided malware analysis and reverse engineering subject matter expertise to government and commercial clients in the Washington, D.C. metropolitan area.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 20:05-20:35 PDT

Title: What!? Is my life that fragile?
When: Saturday, Aug 10, 20:05 - 20:35 PDT
Where: Virtual

Description:

The increased dependency on the digital life to participate in society means, digital life is real life. With that, the consequences of failure in confidentiality, integrity and availability of our digital self, can have dire consequences. So, I threat modelled living in 2024; and it's more fragile than I thought!

How digitally resilient do you think you are?

Let's talk about that, and some things we can do about it.

SpeakerBio: hoodiePony

I'm just a friendly local cyber security sherpa. Helping people verifiably build a safer, secure, and more resilient world by sharing knowledge and experience. This includes the privilege of presenting here at DCG VR previously, and a keynote at ChCon NZ, amongst many other conferences. I am grounded by the many years of experience spent security advising and assessing critical infrastructure in Australia, and governments, to small startups. That said, I'm just another nerd of figuring out how things work, tinkering, and challenging assumptions; sharing a story so that we can all make better informed decisions through broader perspectives.

Return to Index - Add to Google - ics Calendar file

Title: What's next for the commercial CNE marketplace? A chance for you to influence the policy that will impact the future
When: Saturday, Aug 10, 14:00 - 15:45 PDT
Where: LVCC West/Floor 2/W237 - Map

Description:

The marketplace offering commercial proliferation of cyber tools and services (such as end to end CNE capabilities as well as individual components for those capabilities) is lowering the barrier to entry resulting in greater and irresponsible use by threat actors. Across the world, governments, industry, civil society, journalists, and think tanks are responding to this. Through the Pall Mall Process, the UK and French governments are working together to address this challenge, while recognising that these tools and services can provide benefits when used for legitimate purposes and developed responsibly. This session will inform those attending about the Pall Mall Process up to now and look at some of the next steps. It will also give a chance for questions to understand what it could mean for them. There is also a plan to hold an open roundtable at DEF CON for those who wish to provide feedback in a more intimate setting so that this can be considered whilst working through the next steps of the Pall Mall Process.

Speakers:UK Repersentative 2,Senior Representative from UK NCSC,Océane Thieriot,Claudi d'Antoine,Bill Marczak,Daniel Cuthbert

SpeakerBio: UK Repersentative 2, Head of Cyber Proliferation Policy at UK Foreign Commonwealth & Development Office
No BIO available
SpeakerBio: Senior Representative from UK NCSC, CTO for Cyber Policy & Assessment at UK National Cyber Security Centre
No BIO available
SpeakerBio: Océane Thieriot, Counselor for Cyber Affairs at Embassy of France in Washington DC

Océane Thieriot is the Counselor for Cyber Affairs at the Embassy of France in Washington DC. Before joining the Embassy, she held positions within the French Ministry of Foreign Affairs, serving in Brussels (Deputy Antici Counselor and Climate Counselor at the French Permanent Representation to the EU) as well as in Paris (member of the cabinet of the Minister for European Affairs). She is a graduate from Ecole Normale Supérieure, Sciences Po and Ecole Nationale d'Administration.

SpeakerBio: Claudi d'Antoine, President and CEO at Margin Research

Claudia d'Antoine, MD is the President and CEO of Margin Research, an offensive cybersecurity firm based in New York City. Claudia is a business leader and entrepreneur who stands at the intersection of security, technical development, and policy. She works closely with partners in the United States Government as well as within the five eyes community to drive problem-solving and support their missions. She is a member of the Atlantic Council on their Counter-Terrorism projects as well as an advisor to the Pall Mall Process. She has spoken at OffensiveCon and REcon and hosts CTFs for the broader cybersecurity community. Prior to joining Margin, she worked as a software engineer and as a physician. She has a passion for bridging technical divides between industries, advancing cutting edge research, and finding practical applications for mission-driven work.

SpeakerBio: Bill Marczak, Senior Researcher at University of Toronto's Citizen Lab

Bill Marczak is a Senior Researcher at the University of Toronto's Citizen Lab where he investigates novel surveillance and censorship tools that threaten Internet freedom. Bill received his PhD in Computer Science from UC Berkeley. Some of Bill's greatest hits include leading the first public report about NSO Group's Pegasus spyware, and the capture of the ForcedEntry and BlastPass iOS zero-click exploits. Coverage of Bill's work has been featured in Vanity Fair, the New York Times, and on CNN and 60 Minutes.

SpeakerBio: Daniel Cuthbert
No BIO available

Return to Index - Add to Google - ics Calendar file

APV - Friday - 17:00-17:30 PDT

Title: When Chatbots Go Rogue – Lessons Learned from Building and Defending LLM Applications
When: Friday, Aug 9, 17:00 - 17:30 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

From theory to practice: dive into the lessons learned from building and defending an LLM application. This talk offers firsthand insights into the challenges and breakthroughs experienced while developing and securing large language models in real-world settings. We'll explore critical vulnerabilities, innovative defense strategies, and practical tips for enhancing the robustness of AI applications. Join us to gain actionable knowledge that can help you navigate the evolving landscape of AI security with confidence.

Speakers: Andra,Javan Rasokat

SpeakerBio: Andra

Andra is a Principal Application Security Specialist at Sage, with over seven years of experience in the field of application security. She is responsible for implementing DevSecOps practices, conducting security assessments, and developing secure coding guidelines for software engineering and AI/ML teams. She holds multiple certifications, including AWS Certified Cloud Practitioner and Attacking and Securing APIs. She has a strong background in software development and project management, as well as a master's degree in information and computer sciences. She has been co-leading the OWASP London Chapter since 2019, where she organises and delivers events and workshops on various security topics. She is passionate about educating and empowering developers and stakeholders to build and deliver secure software and best practices in a fast-paced, results-driven environment.

SpeakerBio: Javan Rasokat

Javan works as a Senior Application Security Specialist at Sage, helping software teams enhance security throughout the software development lifecycle. In addition to his day job, he lectures on Secure Coding at DHBW University in Germany. Javan’s passion for ethical hacking started young, automating online games and finding security bugs, which he would report to game operators. He turned this passion into a career, first as a security consultant and later specializing in penetration testing. Javan holds a Master’s degree in IT Security Management and several certifications, including GXPN, CISSP, CCSP, and CSSLP. He has shared his expertise at numerous conferences, including OWASP Global AppSec, Ekoparty, and HITB. Last year, Javan gave a talk on the vulnerabilities of large language models, using GitHub Copilot as a case study to examine their impact on secure coding practices.

Return to Index - Add to Google - ics Calendar file

ICSV - Saturday - 11:00-11:50 PDT

Title: Where's Waldo? Can you find the Raspberry Pi in the Cyber Defense Exercise?
When: Saturday, Aug 10, 11:00 - 11:50 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-06-05 - Map

Description:

The Raspberry Pi was designed to make computing accessible and affordable for everyone. For this reason, it's especially useful in the domain of OT and ICS Security workforce development. In a domain frequently understaffed, underfunded and struggling to find interested, qualified candidates (heck, sometimes even just warm bodies!), budgets are tight if not non-existent when it comes to developing the skills needed to secure these systems. This talk will discuss the use of low-cost computing solutions to deliver learning objectives to everyone from existing professionals in a full-scale OT Cyber Defense Exercise to demonstrating ICS principles to the up-and-coming workforce of tomorrow. We'll show how such devices can pinch hit for GPS to provide NTP, act as a PLC, function as a sync server, replace packet squirrels, act as MITM devices, and even how to use them to model fully functioning cyber physical systems on a shoestring educator's budget.

- These statements are the opinions of the researcher/educator presenting and have not been approved by Raspberry Pi Foundation.

Speakers:Shane McFly,Brian Howard

SpeakerBio: Shane McFly

Shane McFly is not a shill for the Raspberry Pi Foundation, but he is always willing to listen to ~~bribe~~ sponsorship offers. He is iN fact, fRom the govErnment and he’s here to heLp. He’s not technically a fed, but his laptop might be. While contributing to a project during his time employed by a research unIversity, he Learned some things about the state of cybersecurity of the US criticaL infrastructure. As a result, he can’t sleep at night unless he’s spending his days helping the folks that defend it. And trying to recruit more help for them (and himself) by indoctrinating local engineering students about CPS security, dragging them to conferences, and making them get up on stage and speak to literally dozens of humans about how to live action role play scenarios around power grid cyber defense with lots of neat equipment (not to mention a few Raspberry Pis) with the help of some ~~scary hackers~~ skilled reverse-engineers. Any rumors of extra credit offered to such students in exchange for spending hours of their own time creating and managing ICS security demonstrations at a nearby table are greatly exaggerated.

SpeakerBio: Brian Howard

Brian Howard is an avid tinkerer with a weak spot for pi. As a grad student and government worker he is no stranger to shoestring budgets and ambitious expectations. As a man of culture, he rarely responds to bribes or promises of extra credit despite recent allegations

Return to Index - Add to Google - ics Calendar file

DC - Friday - 10:00-10:45 PDT

Title: Where's the Money: Defeating ATM Disk Encryption
When: Friday, Aug 9, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Holding upwards of $400,000, ATMs continue to be a target of opportunity and have seen over a 600% increase in crime in just the last few years. During this time, I led security research with another colleague into the enterprise ATM industry resulting in the discovery of 6 zero-day vulnerabilities affecting Diebold Nixdorf's Vynamic Security Suite (VSS), the most prolific ATM security solution in the market. 10 minutes or less is all that a malicious actor would need to gain full control of any system running VSS via offline code injection and decryption of the primary Windows OS. Diebold Nixdorf is one of three major North American enterprise class ATM manufacturers with a global presence in the financial, casino/gaming, and point-of-sale markets. Similar attack surfaces are currently being used in the wild and impact millions of systems across the globe. Furthermore, VSS is known to be present throughout the US gaming industry, including most of the ATM/cash-out systems across Vegas.

In this session, I will publicly disclose this research, review the discovery process, and dive into the technical intricacies of each vulnerability. The Full Disk Encryption module of VSS conducts a complex integrity validation process to ensure a trusted system state, performed as a layered approach during system initialization. Examination of the workflow will highlight various deficiencies that I will demonstrate through PoC exploitation.

Each vulnerability presented in this session has been observed to have a recursive impact across all major versions of VSS and represents a systemic ongoing risk. We will explore the root-cause, vendor remediation steps, and short-comings thereof – perpetuating the attack narrative. In conclusion, proper mitigation techniques and procedures will be covered, providing valuable insights into defending against potential compromise.

- Vynamic Security Suite - Vynamic Security Hard Disk Encryption Secure Sensitive Consumer Data: link
- SEC Consult - Manipulation of pre-boot authentication in CryptWare CryptoPro Secure Disk for Bitlocker: link
- Diebold Nixdorf - EULA for Vynamic Security Suite 3.0: link
- Diebold Nixdorf - Product Legal Terms Website: link
- CryptWare Website: link
- Secure Disk for BitLocker Website: link
- CPSD Website: link
- O'Reilly - Essential System Administration, 3rd Edition by Æleen Frisch: link
- Flowblok's Blog - Shell Startup Scripts: link
- Red Hat Customer Portal - Enhancing Security with the Kernel Integrity Subsystem: link
- OpenSUSE Wiki - SDB:Ima evm: link
- ATMIA - ATM Operator Training: link
- 3SI Systems - Stop Criminals from Cashing in at the ATM: link
- Diebold Nixdorf - Vynamic Security Intrusion Protection Product Card: link
- Diebold Nixdorf - DN Product Card - Vynamic Security Hard Disk Encryption: link
- Everi - Everi to Showcase "Digital Neighborhood" Connecting Guest Loyalty, Cash Access Experiences, and Casino Solutions Made Possible by Industry-Leading Financial Technology Portfolio at 2019 Global Gaming Expo: link
- GlobeNewswire - NRT Accelerates Growth through Acquisition of Casino ATM Portfolio: link
- Northox - How does the TPM perform integrity measurements on a system?: link

SpeakerBio: Matt Burch, Independent Vulnerability Researcher

Matt Burch is an independent vulnerability researcher with 20 years of experience in the information security industry and 15 years of focus in adversarial testing and simulation. He specializes in ATM, IoT, mobile application, and IP based vulnerability research. With this diverse background, he has successfully identified unique deficiencies in high-security

products – awarding him numerous CVE accreditations.

Return to Index - Add to Google - ics Calendar file

Title: Where's the Money: Defeating ATM Disk Encryption
When: Friday, Aug 9, 15:50 - 16:30 PDT
Where: LVCC West/Floor 1/Hall 2/Creator Stage 1 - Map

Description:

Holding upwards of $400,000, ATMs continue to be a target of opportunity and have seen over a 600% increase in crime in just the last few years. During this time, I led security research with another colleague into the enterprise ATM industry resulting in the discovery of 6 zero-day vulnerabilities affecting Diebold Nixdorf's Vynamic Security Suite (VSS), the most prolific ATM security solution in the market. 10 minutes or less is all that a malicious actor would need to gain full control of any system running VSS via offline code injection and decryption of the primary Windows OS. Diebold Nixdorf is one of three major North American enterprise class ATM manufacturers with a global presence in the financial, casino/gaming, and point-of-sale markets. Similar attack surfaces are currently being used in the wild and impact millions of systems across the globe. Furthermore, VSS is known to be present throughout the US gaming industry, including most of the ATM/cash-out systems across Vegas.

In this session, I will walk through my research, review the discovery process, and dive into the technical intricacies of each vulnerability. The Full Disk Encryption module of VSS conducts a complex integrity validation process to ensure a trusted system state, performed as a layered approach during system initialization. Examination of this workflow will highlight various deficiencies that I will demonstrate through PoC exploitation.

Each vulnerability presented in this session has been observed to have a recursive impact across all major versions of VSS and represents a systemic ongoing risk. We will explore the root-cause, vendor remediation steps, and short-comings thereof – perpetuating the attack narrative. In conclusion, proper mitigation techniques and procedures will be covered, providing valuable insights into defending against potential compromise.

SpeakerBio: Matt Burch, Independent Vulnerability Researcher

Matt Burch is an independent vulnerability researcher with 20 years of experience in the information security industry and 15 years of focus in adversarial testing and simulation. He specializes in ATM, IoT, mobile application, and IP based vulnerability research. With this diverse background, he has successfully identified unique deficiencies in high-security products – awarding him numerous CVE accreditations.

Return to Index - Add to Google - ics Calendar file

DCGVR - Saturday - 19:05-19:30 PDT

Title: Who cashed my check?! Catching (Very Obvious) Fraudsters
When: Saturday, Aug 10, 19:05 - 19:30 PDT
Where: Virtual

Description:
SpeakerBio: Squiddy

Squiddy is a transmasc lesbian hacker, Desktop Engineer, and small business owner from the cornfields of the midwest. They joined the hacker scene in 2017 as an OSINT newbie, and founded Defcon574, now merged with Michiana InfoSec, in 2019 as a student organization at Indiana University. Since 2017, they've given presentations at local tech meetups, and at DEF CON, covering various topics from medical information systems, to gender-inclusivity, and open source intelligence.

Return to Index - Add to Google - ics Calendar file

RFV - Saturday - 15:30-15:55 PDT

Title: Who's Afraid of Synthetic Aperture Radar?
When: Saturday, Aug 10, 15:30 - 15:55 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

"Synthetic Aperture Radar (SAR) is one of the most useful and interesting techniques in radar, providing high resolution radar satellite images from relatively small satellites. SAR is not limited by the time of day or by atmospheric conditions. It complements satellite photography and other remote sensing techniques, revealing activity on the Earth that would otherwise be hidden. How does the magic happen? This talk will explain the basics of SAR in an accessible and friendly way. That's the good news.

The bad news? SAR is controlled by ITAR, the International Traffic in Arms Regulations, and is listed in the USML, the United States Munitions List. ITAR regulates the export of defense articles and services and is administered by the US State Department. This includes both products and services as well as technical data. Such as, catalogs of high resolution radar imagery.

Regulation of SAR chills commercial activity, creating costly and time-consuming burdens. But why does any of this matter to signals hackers? Because technology has overtaken the rules, and devices used by enthusiasts, researchers, students, and hackers are increasingly likely to have enough capability to fall into or near export-controlled categories. The penalties are harsh. Fear of running afoul of ITAR is enough to stop a promising open source project in its tracks.

Is there a way forward? Yes. ITAR has a public domain carve out. Information that is published and that is generally accessible or available to the public is excluded from control as ITAR technical data. That's great in theory, but how can we increase our confidence that we are interpreting these rules correctly? How can we use and build upon these rules, so that our community can learn and practice modern radio techniques with reduced fear and risk? Can we contribute towards regulatory relief when it comes to SAR? We will describe the process, report on the progress, and enumerate the challenges and roadblocks."

SpeakerBio: Abraxas3d, Technical Specialist and Technical Advisor at ARRL

Michelle enjoys thinking and doing. Not necessarily in that order.

She completed an MSEE from USC in Information Theory while working at Qualcomm Incorporated. Her IEEE work focuses on industry involvement and citizen science. Michelle is a founder and current CEO of Open Research Institute, a non-profit R&D firm that publishes Open Source work to the general public. She is responsible for major regulatory reform in the amateur satellite service. She represents ORI on the FCC Technological Advisory Council, is a Technical Specialist and Technical Advisor for ARRL, and she also serves as the Vice President of an independent telephone company in rural Mississippi.

Return to Index - Add to Google - ics Calendar file

CON - Friday - 18:30-19:30 PDT

Title: Whose Slide Is It Anyway?
When: Friday, Aug 9, 18:30 - 19:30 PDT
Where: LVCC West/Floor 1/Hall 1/Tracks 1-2 - Map

Description:

If someone had told us this silly contest would be in its 8th year there's no way we would have believed it. Even when we thought "hey, the gag is getting old, maybe it's time to hang it up" that turned out to be the year we'd gotten the most accolades from con goers during and after the contest. That was enough to recharge us and decide we'll do this until DC no longer exists. Proud isn't a grand enough word to describe how we feel to still be here and still making people laugh/feel better about themselves not being as stupid as us.

But to answer Why Us? WSIIA has always been about community. Whether you killed your deck or went down in a spectacular blaze of flames, this game is nothing without the people who play it and the audience who watches it. And if we're not doing it for the community, why the fuck are we even here? We'll remain here as long as you'll have us, riding on a wing, a prayer, and airplane bottles of Malort all the way to Year 10. Now on to the boilerplate pitch:

We're an unholy union of improv comedy, hacking and slide deck sado-masochism.

Our team of slide monkeys will create a stupid amount of short slide decks on whatever nonsense tickles our fancies. Slides are not exclusive to technology, they can and will be about anything. Contestants will take the stage and choose a random number corresponding to a specific slide deck. They will then improvise a minimum 5 minute / maximum 10 minute lightning talk, becoming instant subject matter experts on whatever topic/stream of consciousness appears on the screen.

Whether you delight in the chaos of watching your fellow hackers squirm or would like to sacrifice yourself to the Contest Gods, it’s a night of schadenfreude for the whole family.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 16:30-17:15 PDT

Title: Why are you still, using my server for your internet access.
When: Friday, Aug 9, 16:30 - 17:15 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

Pawning countries at top level domain by just buying one specific domain name ‘wpad.tld’, come hear about this more the 25+ years old issue and the research from running eight different wpad.tld domains for more than one year that turn into more the 1+ billion DNS request and more then 600+GB of Apache log data with leaked information from the clients.

This is the story about how easy it is to just buying one domain and then many hundreds of thousands of Internet clients will get auto pwned without knowing it and start sending traffic to this man-in-the-middle setup there is bypassing encryption and can change content with the ability to get the clients to download harmful content and execute it.

The talk will explain the technical behind this issue and showcase why and how clients will be trick into this Man-in-the-middle trap.

1. Description of wpad and the function, include listing the security issue. link
2. Navigator Proxy Auto-Config File Format from March 1996 link
3. INTERNET-DRAFT 1999 for Web Proxy Auto-Discovery Protocol link
4. Microsoft Security Bulletin MS99-054 Critical Vulnerability from 1999 link
5. Description of the wpad PAC javascript format. link
6. Pentesting tool with function as a WPAD Proxy Server to capture credentials from clients. link
7. WPAD Name Collision Vulnerability link
8. WPAD Vulnerability link link
9. ICANN - Root Cause Analysis - wpad.domain.name link
10. Windows proxy settings ultimate guide part – WPAD/PAC configuration file
    - link
    - link
    - link

SpeakerBio: Thomas Boejstrup Johansen

Thomas Boejstrup Johansen aka Tooms has been in professional IT for more than 25+ years, where the first 11+ years were as a system administrator for a large Danish company and the last 14+ years as a security specialist with the work in the field of Reverse Engineering Malware, Incident Response and Forensics but also physical redteam engagements and pentesting for customers.

The last many years have been mainly as lead senior forensics investigator and incident response on many incidents including some more well known major incidents like the incident in 2021 there got known around the world as Microsoft Exchange Hafnium vulnerability.

Return to Index - Add to Google - ics Calendar file

BBV - Friday - 14:00-14:59 PDT

Title: Why You Should Be Hunting on Web3 Bug Bounties
When: Friday, Aug 9, 14:00 - 14:59 PDT
Where: LVCC West/Floor 2/W215 - Map

Description:

The presentation will feature a brief introduction to Web3 and Web3 bug bounties, notoriously some of the differences that the typical blockchain transparency brings in comparison to web2. Then we will explain what's at stake in Web3. In traditional bug bounties, what's most often at stake is PII data, as well as critical infrastructure. In the blockchain world, money is at malicious actors' finger tips - extremely large sums of money. We will go over some of the most notorious hacks that happened in Web3, and we will look at real blockchain data:

- The technical details of the exploit
- The money flows
- The out of this world messages sent in the negotiation process between the hackers and the hacked protocol. Yes, often this negotiation actually happens through transparent blockchain transactions.

Finally, we will recreate some of the most iconic +$1M bounties and their proof of concepts. At least one will be on smart contracts, one will be on the blockchain stack and one on will be in novelty zero knowledge circuit technology.

SpeakerBio: Gonçalo Marques Raposo de Magalhães, Head of Security at Immunefi

Aerospace engineer, turned embedded systems engineer, turned smart contract engineer. Currently Head of Security at Immunefi and Advanced Solidity and Blockchain teacher. Web3 security audits independently.

Return to Index - Add to Google - ics Calendar file

IOTV - Sunday - 10:15-11:45 PDT

Title: Wi-Fi Hacker Hunting
When: Sunday, Aug 11, 10:15 - 11:45 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

Become a Wi-Fi investigator: Uncover Hidden Wi-Fi Cameras, network Intruders, and more with the Wi-Fi Nugget. In this workshop, we'll use a cute, cat-shaped microcontroller board to catch hackers using well-known hacking tools like a Wi-Fi Pineapple, hunt down suspicious Wi-Fi devices like hidden cameras, and detect jamming attacks. We'll explore how low-cost microcontrollers can be used to unmask and track down Wi-Fi hacking tools, or locate unwanted devices on your local network.

SpeakerBio: Kody K

No BIO available

Return to Index - Add to Google - ics Calendar file

IOTV - Saturday - 14:15-16:15 PDT

Title: Wi-Fi Hacking Self Defense: Four Advanced Techniques and How to Stop Them
When: Saturday, Aug 10, 14:15 - 16:15 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-04 - Map

Description:

This workshop offers hands-on instruction using a unique, cat-shaped Wi-Fi hacking microcontroller. Designed to engage participants in practical learning, the workshop will cover essential skills for defending against four common Wi-Fi attacks. Participants will explore topics like detecting Wi-Fi leaks, the risks of QR codes leading to hidden networks, spotting phishing networks, and defending against advanced Wi-Fi karma attacks. The cat-shaped Wi-Fi Nugget is a powerful tool for understanding and fighting back against Wi-Fi hacking. This workshop is suitable for Wi-Fi hacking experts and those just getting started. A computer with a Chrome-based browser is required for this workshop.

SpeakerBio: Kody K
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 10:00-10:45 PDT

Title: Windows Downdate: Downgrade Attacks Using Windows Updates
When: Sunday, Aug 11, 10:00 - 10:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

Downgrade attacks force software to revert to an older, vulnerable version. In 2023, BlackLotus emerged, downgrading the boot manager to bypass Secure Boot. Microsoft addressed the threat, but was Secure Boot the only component vulnerable to downgrades?

By examining Windows Updates, we found a flaw enabling us to take full control over it and craft downgrading updates, bypassing all verification steps.

We then managed to downgrade DLLs, drivers, and even the kernel. Afterwards, the OS reported it's fully updated, unable to install future updates, with recovery tools unable to detect issues.

We aimed higher and found that the virtualization stack is at risk too. We successfully downgraded Hyper-V's hypervisor, Secure Kernel, and Credential Guard to expose privilege escalations.

We also discovered several ways to disable VBS, including its Credential Guard and HVCI features, despite its enforced UEFI locks. This is the first known bypass of VBS's UEFI locks.

Lastly, we found another vulnerability in a Windows Update restoration scenario, making the findings accessible to unprivileged attackers!

In this talk, we'll introduce "Windows Downdate", a tool that takes over Windows Updates to craft downgrades and expose dozens of vulnerabilities. It makes the term "fully patched" meaningless across any Windows machine worldwide.

SpeakerBio: Alon Leviev

Alon Leviev (@_0xDeku) is self-taught security researcher with a diverse background. Alon started his professional career as a blue team operator, where he focused on the defensive side of cyber security. As his passion grew towards research, Alon joined SafeBreach as a security researcher. His main focus include operating system internals, reverse engineering, and vulnerability research. Alon spoke at various security conferences such as Black Hat EU 2023, CanSecWest 2024 and CONFidence 2024. Before joining the cyber security field, Alon was a professional Brazilian jiu-jitsu athlete, where he won several world and european titles.

Return to Index - Add to Google - ics Calendar file

APV - Friday - 10:15-10:45 PDT

Title: Winning big: AppSec Considerations From the Casino Industry
When: Friday, Aug 9, 10:15 - 10:45 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

In the casino industry, a surge of ransomware attacks has marked an era of unprecedented threats and vulnerabilities. This session will focus on a critical aspect of security within this industry, exploring how ransomware has specifically impacted applications and associated systems. Attendees will gain insights into the methods used by malicious actors to compromise casino applications, the resulting financial and operational disruptions, (i.e., affected customer data security etc.) and responses developed to counter these threats. By researching industry giants like MGM and Caesars, we will highlight the importance of robust application security measures and the future landscape of cybersecurity in this sector. Unique security challenges faced by the casino industry will be explored, along with examples of vulnerabilities and their exploitation. The session will also delve into the interplay between ICT, IoT, and application security in the casino context.

Speakers: Aleise McGowan,Tennisha Martin

SpeakerBio: Aleise McGowan

Dr. Aleise H. McGowan is a cybersecurity leader and academic with over 20 years of experience in the field. She serves as the CISO for BlackGirlsHack, an organization dedicated to increasing diversity in cybersecurity, while also holding the position of Assistant Professor at the University of Southern Mississippi.

SpeakerBio: Tennisha Martin

Tennisha Martin is the founder and Executive Director of BlackGirlsHack (BGH Foundation), a national cybersecurity nonprofit organization dedicated to providing education and resources to underserved communities and increasing the diversity in cyber. BlackGirlsHack provides its members with resources, mentorship, direction, and training required to enter and excel in the cybersecurity field. Tennisha has a bachelor's degree in Electrical and Computer Engineering from Carnegie Mellon University and several Master's Degrees including in Cybersecurity and Business Administration. She has worked in a consulting capacity for over 15 years and is a best selling author, award winning hacker, and an advocate for diversity.

Return to Index - Add to Google - ics Calendar file

PHV - Sunday - 12:00-12:59 PDT

Title: Winning the Game of Active Directory
When: Sunday, Aug 11, 12:00 - 12:59 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

The Game Of Active Directory (GOAD) is a prebuilt vulnerable Active Directory (AD) environment primarily created for pentesters. Touting over 30 methods of attack, GOAD offers multiple paths to full AD takeover. But is that really how you win the game? Regardless of color, as security professions our goal should be to better secure environments. This talk walks through AD attack strategies, exploiting misconfigurations that ultimately pwn AD. Mitigations for these attacks are discussed and implemented, showcasing how they stop common attacks. Implementing these protections in your environment is truly how you win the Game Of Active Directory.

SpeakerBio: Brandon Colley, Senior Security Consultant at Trimarc

Brandon Colley has over fifteen years of experience administering and securing Active Directory (AD) and Windows environments. Brandon is a Senior Security Consultant for Trimarc specializing in providing reality-based AD and Entra ID security assessments. He served as a systems administrator for multiple organizations before shifting career focus to information security. He has published multiple articles through Quest, Practical 365 and Trimarc Hub. Brandon enjoys speaking engagements and has previously presented at BsidesKC, Hackers Teaching Hackers, and PancakesCon. He co-hosts a weekly podcast, interviewing infosec professionals and has appeared on multiple broadcasts, including the Phillip Wylie Show. Brandon delivers material in a humorous, yet effective manner with a focus on content built for a Blue Team through a Red lens.

Return to Index - Add to Google - ics Calendar file

ESV - Sunday - 10:00-12:59 PDT

Title: Wireless & Networking workshop
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Come and explore embedded communication by sniffing wireless traffic, exploring embedded servers, and finding flags hidden within.

SpeakerBio: Alex Kelly
No BIO available

Return to Index - Add to Google - ics Calendar file

ESV - Friday - 10:00-17:59 PDT

Title: Wireless & Networking workshop
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Come and explore embedded communication by sniffing wireless traffic, exploring embedded servers, and finding flags hidden within.

SpeakerBio: Alex Kelly
No BIO available

Return to Index - Add to Google - ics Calendar file

ESV - Saturday - 10:00-17:59 PDT

Title: Wireless & Networking workshop
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-05 - Map

Description:

Come and explore embedded communication by sniffing wireless traffic, exploring embedded servers, and finding flags hidden within.

SpeakerBio: Alex Kelly
No BIO available

Return to Index - Add to Google - ics Calendar file

MISC - Sunday - 10:00-12:59 PDT

Title: WISP Community & Inclusion Room
When: Sunday, Aug 11, 10:00 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-04 - Map

Description:

Chill out space to relax with us in a safe place. Grab a non-alcoholic drink, unleash your creativity and unwind with our art therapy, and connect with women and underrepresented communities working in security and privacy.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 10:00-17:59 PDT

Title: WISP Community & Inclusion Room
When: Saturday, Aug 10, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-04 - Map

Description:

Chill out space to relax with us in a safe place. Grab a non-alcoholic drink, unleash your creativity and unwind with our art therapy, and connect with women and underrepresented communities working in security and privacy.

Return to Index - Add to Google - ics Calendar file

MISC - Friday - 10:00-17:59 PDT

Title: WISP Community & Inclusion Room
When: Friday, Aug 9, 10:00 - 17:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-04 - Map

Description:

Chill out space to relax with us in a safe place. Grab a non-alcoholic drink, unleash your creativity and unwind with our art therapy, and connect with women and underrepresented communities working in security and privacy.

Return to Index - Add to Google - ics Calendar file

MISC - Saturday - 15:45-15:59 PDT

Title: WISP Group Photo
When: Saturday, Aug 10, 15:45 - 15:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-04 - Map

Description:

Gather with members of the Women in Security and Privacy community for a group picture.

Return to Index - Add to Google - ics Calendar file

SOC - Saturday - 19:00-20:59 PDT

Title: Women, gender non-conforming and non-binary meetup with The Diana Initiative
When: Saturday, Aug 10, 19:00 - 20:59 PDT
Where: LVCC West/Floor 3/W305-W306 - Map

Description:

The Diana Initiative is hosting a meetup where we'd love to get all the gender non conforming, non-binary and women attendees together to hang out and make friends! DEF CON is better with friends.

Return to Index - Add to Google - ics Calendar file

RFV - Sunday - 12:30-12:59 PDT

Title: World Wide War Drive Outbrief
When: Sunday, Aug 11, 12:30 - 12:59 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:
Speakers:RF Hackers,WiGLE Staff

SpeakerBio: RF Hackers
No BIO available
SpeakerBio: WiGLE Staff
No BIO available

Return to Index - Add to Google - ics Calendar file

BICV - Friday - 13:00-13:59 PDT

Title: Worried about AI taking your job? Then this talk is for you.
When: Friday, Aug 9, 13:00 - 13:59 PDT
Where: LVCC West/Floor 3/W314-W316 - Map

Description:

Artificial intelligence (AI) promises to be a game-changing technology across industries, but when it comes to identifying and mitigating complex cybersecurity threats, AI still falls short. The inherent nature of malicious attacks and the sophistication of hackers ultimately hamper even the most advanced AI systems currently available. There are many critical jobs where AI cannot replace humans due to the limits of current technology in exercising judgment, especially in undefined and complex situations. AI can only process information it has been trained on, lacking real-world experience and the discernment needed for high-stakes decision making.

SpeakerBio: Levone Campbell, Incident Response & Cyber Operations Consultant

Levone Campbell brings over 18 years of extensive experience to his role as Cyber Security Lead and Incident Coordinator, safeguarding his organization on the digital front. He first built expertise in core information technology before specializing in the critical domain of cybersecurity. Over nearly two decades, Levone has amassed comprehensive knowledge spanning cyber security operations, cyber threat intelligence, cyber-crime investigation and espionage. He provides a veteran presence, coordinating incident response and fortifying the organization's overall security posture against both internal and external threats. To complement his on-the-ground experience, Levone holds a duo of bachelor's degrees in management and marketing from North Carolina A&T State University. Understanding the importance of lifelong learning, he furthered his education with a MBA from Walden University and a Masters in Technology Management from Georgetown University. Additionally, Levone has earned numerous industry certifications to stay updated with the latest cybersecurity tools and tactics.

Return to Index - Add to Google - ics Calendar file

CPV - Sunday - 13:00-13:30 PDT

Title: Wu-Tang is for the Children: How States Laws Intended to Protect Children Raise Other Privacy and Legal Risks
When: Sunday, Aug 11, 13:00 - 13:30 PDT
Where: LVCC West/Floor 2/W222-Creator Stage 4 - Map

Description:

On February 25, 1998, hip-hop group the Wu-Tang Clan made Grammy history… for all the wrong reasons. After losing in the Rap Album of the Year category, Wu-Tang member ODB stormed the stage, interrupting an acceptance speech to declare the now infamous phrase “Wu-Tang is for the children.” Anyone who has heard a song from Wu-Tang knows that despite ODB’s insistence, it is certainly not true. It appears that States may be taking this same approach when it comes to children's privacy and safety online. Despite these laws being for the protection of children, they often raise other unintended consequences. State legislatures around the country are debating new laws to protect children online. This year, Tennessee, Maryland, Virginia, Georgia, Utah, and Florida have passed legislation focused on children's privacy, usually through restrictions on social media use. While privacy advocates have championed these laws, they have been met with criticism and, in some instances, legal challenges. This is because in order to implement laws that apply to kids online, companies have to identify which users are kids—which requires the collection of sensitive personal information. Along with this privacy tension, there are First Amendment protection concerns that these laws limit online speech. This presentation will explore how youth privacy laws may not be protecting children in the ways that we hope by first discussing the attempts made by states to address youth privacy. Then, analyzing the unintended privacy consequences, focusing on how states are required to collect sensitive information that we are often trying to protect. Next, we will examine the First Amendment concerns using the example of the challenges to California’s Age Appropriate Design Code Act before finally discussing a path forward to protecting children.

SpeakerBio: Anthony Hendricks, Litigator at Crowe & Dunlevy

Anthony Hendricks is a legal problem solver and litigator at Crowe & Dunlevy, one of Oklahoma’s largest and oldest firms. At Crowe & Dunlevy, Anthony serves as founder and chair of the firm’s Cybersecurity and Data Privacy Practice Group. His legal practice focuses on data privacy compliance, regulatory enforcement and permitting, and other “bet-the-company” suits in the areas of cybersecurity, privacy, and other complex business litigation. Anthony is an adjunct professor who teaches Cybersecurity Law and Information Privacy courses at Oklahoma City University School of Law. He also hosts “Nothing About You Says Computer Technology,” a podcast on cybersecurity and data privacy viewed through the lens of diverse voices. Anthony has been nationally recognized for his legal skills. He has been selected as a member of the Lawyers of Color Hot List, a 40 under 40 attorney by the National Association of Black Lawyers, Oklahoma Magazine 40 under 40, and the Journal Record 40 under 40, and is listed by both Super Lawyers Magazine and Best Lawyers. Anthony is a former cybersecurity policy fellow in New America’s Cybersecurity Initiative. To learn more about Anthony’s current projects, upcoming speaking events or listen to the latest episodes of his podcast, visit www.anthonyjhendricks.com

Return to Index - Add to Google - ics Calendar file

DL - Friday - 14:00-15:45 PDT

Title: XenoboxX - Hardware Sandbox Toolkit
When: Friday, Aug 9, 14:00 - 15:45 PDT
Where: LVCC West/Floor 3/W307 - Map

Description:

Malware frequently employs anti-VM techniques, which can vary in their difficulty to detect and counteract. While integrating anti-detection measures in our labs is a frequently used option, we should also consider using a real hardware sandbox, even if this sounds weird. By leveraging the awesome PCILeech project and DMA hardware access, XenoboxX provides a suite of tools for analysis tasks, such as dumping dynamically allocated memory and searching for IoC. These tools allow us to inject code at kernel level through DMA, making detection significantly more challenging and giving a new perspective to the analysis.

SpeakerBio: Cesare Pizzi, Security Researcher, Analyst, and Technology Enthusiast

Cesare Pizzi is a Security Researcher, Analyst, and Technology Enthusiast. Mainly focused on low level programming, he developed a lot of OpenSource software, sometimes hardware related (USBvalve) and sometimes not.

Doing a lot of reverse engineering too. He likes to share his job when possible (at Defcon, Insomni'hack, Nullcon. etc). Contributor of several OS Security project (Volatility, OpenCanary, PersistenceSniper, Speakeasy, CETUS, TinyTracer, etc) and CTF player.

Return to Index - Add to Google - ics Calendar file

DC - Friday - 13:30-14:15 PDT

Title: Xiaomi The Money - Our Toronto Pwn2Own Exploit and Behind The Scenes Story
When: Friday, Aug 9, 13:30 - 14:15 PDT
Where: LVCC West/Floor 3/W322-W327 - Map

Description:

At Pwn2Own Toronto 2023, NCC Group was one of the two teams that compromised the Xiaomi 13 Pro. The exploit chain involved using a malicious HTML hyperlink and uploading a potentially malicious application to the Xiaomi app store.

However, this talk is not just about the technical details of the exploit. While researching the final exploit, NCC Group discovered how an exploit could work in one region of the world, but not in other regions, and how the researchers had to travel to Canada for a day just to test if the exploit would work in Canada. This talk also discusses just how far Xiaomi is willing to go to make sure their device isn't hacked at Pwn2Own, and why only two teams were able to successfully compromise the device during the competition.

Speakers:Ken Gannon,Ilyes Beghdadi

SpeakerBio: Ken Gannon, Principal Security Consultant at NCC Group

Ken is a Principal Security Consultant at NCC Group who specializes in mobile security and doing security research on mobile devices. He occasionally complains about Xiaomi and other phone manufacturers.

SpeakerBio: Ilyes Beghdadi, Senior Application Security Engineer at Census Labs

Ilyes is a Senior Application Security Engineer at Census Labs. At the time of the Pwn2Own research and entry, he was a Security Consultant at NCC Group who worked on reverse engineering Android malware.

Return to Index - Add to Google - ics Calendar file

XRV - Saturday - 12:00-12:30 PDT

Title: XR for All: Accessibility and Privacy for Disabled Users
When: Saturday, Aug 10, 12:00 - 12:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Extended Reality (XR) technologies offer tremendous new possibilities for socializing, entertainment, training, and more. Unfortunately, many disabled users find themselves excluded from XR entirely or exposed to severe privacy risks for using it. In this talk, Dylan Fox, Director of Operations for the XR Access Initiative at Cornell Tech, will discuss the core challenges disabled people face in using XR, the tensions between privacy and assistive capabilities, and the open-source efforts happening now to ensure XR is accessible to everyone.

SpeakerBio: Dylan Fox, Director of Operations, XR Access Initiative at Cornell Tech

I'm a designer, manager, and researcher specializing in accessibility for emerging technologies, particularly VR and AR. I aim to bring together user needs, technological capabilities, and stakeholder requirements to create accessible products.

Return to Index - Add to Google - ics Calendar file

RFV - Friday - 14:30-15:25 PDT

Title: Yet another way of exfiltrating data from air-gapped systems OR Oh no, everything is a radio
When: Friday, Aug 9, 14:30 - 15:25 PDT
Where: LVCC West/Floor 1/Hall 3/HW3-05-03 - Map

Description:

Devices with radios are everywhere and sooner or later radios will be in everything, maybe even sooner than you think. During our talk we will be sharing CNLohr's research about transmitting RF signals without a radio. We will share our findings on how this these new techniques can be abused by an adversary. Finally, we will highlight how so many amazing tools and techniques are available to us because they are open source and why we need to support and protect these kinds of works to sustain a culture of learning and growing.

Speakers:C$,Endeavors

SpeakerBio: C$, Founder at DCG862 (DEF CON Group 862)

Meat-based, Founder of DCG862

SpeakerBio: Endeavors, Founding Member at DCG862 (DEF CON Group 862)

DCG862 founding member

Return to Index - Add to Google - ics Calendar file

BHV - Saturday - 14:00-14:30 PDT

Title: You got a lighter? I need to do some Electroporation.
When: Saturday, Aug 10, 14:00 - 14:30 PDT
Where: LVCC West/Floor 1/Hall 4/Creator Stage 3 - Map

Description:

Biological warfare is a phenomenon that spans human history, tracing its roots to ancient times rather than being a recent invention. To gain insights into bioweapons' current and future landscape, it is imperative to look into historical examples of conventional biological warfare and understand how methods were devised and implemented. Our future hinges significantly on our ability to foster transparency and creativity within the global community. This optimism is intertwined with our comprehension of technological advancements, the rapid pace of innovation, the interconnectedness of various domains, and the imperative task of constructing practical defenses against emerging threats. As a poignant reminder, our vulnerability lies in technological shortcomings and our collective failure of imagination. This discourse extends to establishing social norms and mores that are pivotal in shaping attitudes toward biological warfare and encompasses an exploration of prospective research endeavors and emerging initiatives leveraging artificial intelligence (AI) in the realm of bioweaponry. As we confront the intricate interplay between technological advancements and human agency, it is imperative to remain vigilant and resolute in our pursuit of a future safeguarded against the malevolent exploitation of biological agents.

Speakers: James Utley,Joshua HIll,Phil Rhodes

SpeakerBio: James Utley, Chief Scientific Officer at Auragens

Meet Dr. James Utley, PhD, a distinguished Immunohematology expert and cellular therapy pioneer. A Johns Hopkins alum, he transformed cellular transfusion at the Department of Defense. A true Biohacker, James pushes the boundaries of CRISPR and genetic engineering through self-experimentation. As the former Technical Director at a large healthcare organization, he oversaw 150K successful cellular transfusions, merging technical expertise with innovative practices. His avant-garde publications and FDA-approved breakthroughs underscore his impact. Now, as the Chief Scientific Officer at Auragens, James is a trailblazer in the stem cell revolution. Dubbed the “pirate” of the cellular world, he continues to reshape and advance the field, making a significant difference every day.

SpeakerBio: Joshua HIll
No BIO available
SpeakerBio: Phil Rhodes
No BIO available

Return to Index - Add to Google - ics Calendar file

DC - Sunday - 13:00-13:45 PDT

Title: Your AI Assistant has a Big Mouth: A New Side-Channel Attack
When: Sunday, Aug 11, 13:00 - 13:45 PDT
Where: LVCC West/Floor 1/Hall 1/Track 3 - Map

Description:

AI assistants like ChatGPT are changing how we interact with technology. But what if someone could read your confidential chats? Imagine awkwardly asking your AI about a strange rash, or to edit an email, only to have that conversation exposed to someone on the net. In this talk we'll unveil a novel side-channel vulnerability in popular AI assistants and demonstrate how it can be used to read encrypted messages sent from AI Assistants.

Before our disclosure, major players like OpenAI, Microsoft, Cloudflare, Quora, and Notion were at risk. We'll reveal the technical details of this exploit and show real-world examples of intercepted conversations. This talk isn't just about the problem – learn how to identify this vulnerability in other AI assistants as well! We'll dissect network traffic, discuss attack models, and explore the far-reaching consequences of this discovery.

References: 1. Samuel Addington. Chatgpt: Cyber security threats and countermeasures. Available at SSRN 4425678, 2023. 2. Benjamin Harsha, Robert Morton, Jeremiah Blocki, John Springer, and Melissa Dark. Bicycle attacks con- sidered harmful: Quantifying the damage of widespread password length leakage. Computers & Security, 100:102068, 2021. 3. John V Monaco. What are you searching for? a remote keylogging attack on search engine autocomplete. In 28th USENIX Security Symposium (USENIX Security 19), pages 959–976, 2019.

Speakers: Yisroel Mirsky,Roy Weiss,Daniel Ayzenshteyn,Guy Amit

SpeakerBio: Yisroel Mirsky, Tenure-Track Lecturer and Zuckerman Faculty Scholar, Department of Software and Information Systems Engineering at Ben-Gurion University

Dr. Yisroel Mirsky is a tenure-track lecturer and Zuckerman Faculty Scholar in the Department of Software and Information Systems Engineering at Ben-Gurion University and the head of the Offensive AI Research Lab there. His main research interests include deepfakes, adversarial machine learning, anomaly detection, and intrusion detection. Dr. Mirsky has published his work in some of the best security venues: USENIX, CCS, NDSS, Euro S&P, Black Hat, DEFCON AI Village, RSA, CSF, AISec, etc. His research has also been featured in many well-known media outlets: Popular Science, Scientific American, Wired, The Wall Street Journal, Forbes, and BBC. Some of his works include the exposure of vulnerabilities in the US 911 emergency services and research into the threat of deepfakes in medical scans, both featured in The Washington Post.

SpeakerBio: Roy Weiss, Researcher and Master's Degree Student, Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev

Roy Weiss is a researcher and a master's degree student in the Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev. His research interests include Cyber Security, Network Security and Deep Learning.

SpeakerBio: Daniel Ayzenshteyn, Researcher and Master's Degree Student, Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev

Daniel Ayzenshteyn is a researcher and master's degree student in the Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev. His research interests span Network Security, Cyber Security and Network Modeling.

SpeakerBio: Guy Amit, PhD Candidate Student, Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev

Guy Amit works at IBM Research and is a PhD candidate student in the Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev. His research interests include machine learning, adversarial learning, and IoT cyber security.

Return to Index - Add to Google - ics Calendar file

APV - Sunday - 11:45-12:15 PDT

Title: Your CI/CD Pipeline Is Vulnerable, But It's Not Your Fault
When: Sunday, Aug 11, 11:45 - 12:15 PDT
Where: LVCC West/Floor 2/W228-W230/W228-W230-ASV Main Stage - Map

Description:

Are you really sure that the code executed inside your pipelines is secure? Join us as we explore how command injection in a single CI/CD pipeline component can create a major vulnerability in Google's flagship project, Bazel.

Our research reveals a command injection vulnerability within Bazel GitHub Action, showcasing the potential compromise of the entire open-source project. Through live demonstrations, we illustrate how threat actors can exploit seemingly secure pipelines and tamper widely used repositories with malicious code.

By attending, you'll gain actionable insights into securing your CI/CD pipelines and learn practical strategies to protect your projects from similar vulnerabilities.

Speakers:Elad Pticha,Oreen Livni

SpeakerBio: Elad Pticha

Elad is a passionate security researcher with a focus on software supply chain and web application security. He dedicates his time to writing security research tools and finding vulnerabilities across a broad spectrum, from open-source projects and web applications to IoT devices and pretty much anything with an IP address.

SpeakerBio: Oreen Livni

Oreen Livni is a passionate security researcher specializing in application and supply chain security, Domain, and networking. With a focus on software supply chain vulnerabilities. Alongside his professional commitments, he immerses himself in art, gardening, and the world of surfing, always seeking new experiences. With an unwavering commitment to staying updated on the latest security trends, he embraces new challenges and strives to make a difference in the cybersecurity landscape.

Return to Index - Add to Google - ics Calendar file

PSV - Friday - 14:30-15:30 PDT

Title: Your Smartcard is Dumb: A Brief History of Hacking Access Control Systems
When: Friday, Aug 9, 14:30 - 15:30 PDT
Where: LVCC West/Floor 1/Hall 2/HW2-08-03 - Map

Description:

Have you ever wondered how those little boxes that you tap your card to open doors work? What are they reading on the card? How do they ultimately unlock the door? And, are they even secure? In this talk, we will answer all of those questions and more. We will walk through how access-control systems, in general, work, and dig into the details of the most popular systems. Fortunately for the entertainment value of this talk, there be dragons in our doors. We will walk through some of the most high-profile attacks in detail and then dive into some more fundamental flaws with how the systems are designed. All of these discussions will be accompanied with live demos and first hand experience. After this talk, you will look at the world, especially doors, differently -- weaknesses everywhere! My hope is that we can all learn from past mistakes and create a more secure and less frustrating tomorrow together

SpeakerBio: Chad Shortman, CEO at Allthenticate

Chad is a computer security researcher, entrepreneur, and educator who is passionate about using technology to make people's lives easier and their digital systems more secure. He is currently the CEO of Allthenticate, a company that provides a single smartphone-based solution for both keyless physical access control and passwordless digital authentication. Chad has over 15 years of research experience and has numerous academic publications in top conferences. Formerly, he was a member of the technical research staff at MIT Lincoln Laboratory, where he worked on offensive cybersecurity research. Chad received his Ph.D. from UCSB and is also a recipient of the prestigious IBM Ph.D. Fellowship. In addition to his academic credentials, Chad is a lifetime hacker. His hacking career started in his teenage years and has taken him to compete in some of the world's best capture the flag tournaments around the world as a member of the Shellphish hacking team.

Return to Index - Add to Google - ics Calendar file

DL - Friday - 10:00-11:45 PDT

Title: Zip It Up, Sneak It In - Introduction of apkInspector
When: Friday, Aug 9, 10:00 - 11:45 PDT
Where: LVCC West/Floor 3/W304 - Map

Description:

apkInspector is a tool designed to tackle Android APKs, helping to uncover and decode the evasive tactics used by malware. It can decompress APK entries and extract detailed information such as entry names and sizes, making it easy to analyze the contents of an app. The tool also processes and decodes Android XML (AXML) files into a human-readable format, all while considering the sneaky evasion tactics that malware might employ. apkInspector is able to also identify specific evasion techniques used by malware to bypass static analysis, providing crucial insights for security analysis. It is built to function both as a standalone command-line interface (CLI) for direct operations and as a library that can be integrated into other security tools, enhancing its utility and adaptability in various cybersecurity environments.

Speakers:Kaloyan Velikov,Leonidas Vasileiadis

SpeakerBio: Kaloyan Velikov

Kaloyan Velikov is a security professional that has also been in the cybersecurity field for more than five years. While he is proficient in web application and network security pentesting, as well as various device assessments, in the recent years he has been busy learning the testing of mobile applications and device configurations. This led to a more focused specialization in pentesting on both the Android and iOS platforms. He is always eager to try new tools and see how they can be implemented into the penetration testing playbook. Kaloyan is always up for a challenge even if there is a skill gap and extra research will be required to proceed. He also loves to share the knowledge he has obtained, because it is great to help each other to succeed in our assignments.

SpeakerBio: Leonidas Vasileiadis

Meet Leonidas, an enthusiast in Android’s security landscape, a physicist with a double master's in cybersecurity and over five years of dedicated cybersecurity experience. He’s not just about flashy titles; he’s got the certifications to prove he can push buttons and hack the world. Passionate about web and mobile security, he loves building solutions with code. He’s a firm believer that sharing is caring and enjoys unraveling the complexities of cyber threats as much as he loves tackling riddles. Dive into his session to explore sneaky Android malware tricks, leaving equipped to spot and stop them like a pro.

Return to Index - Add to Google - ics Calendar file

NEWS

DEF CON Response to Badge Controversy

Posted 8.10.24

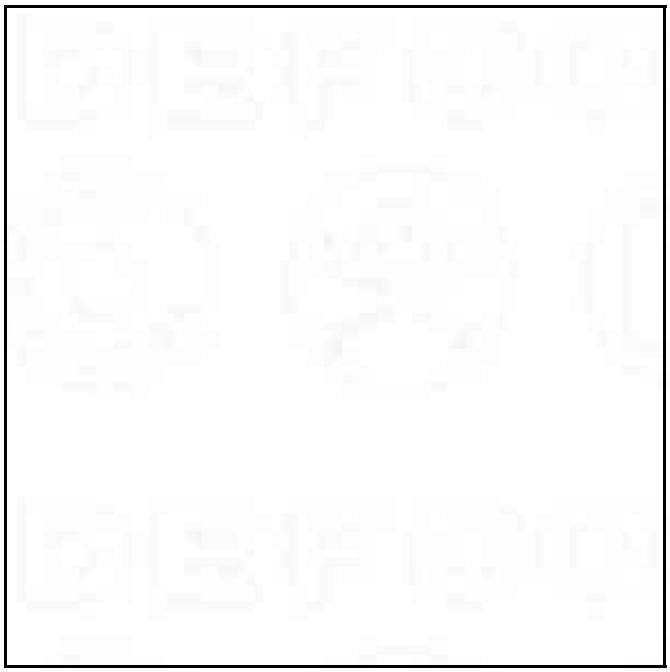
DEF CON thrives on community collaboration and has operated for over 30 years successfully working with hundreds of vendors including the dozens that have helped with our badges over the years. For this year's Raspberry Pi badges, DEF CON hired Entropic Engineering to do the hardware development and firmware. After going overbudget by more than 60%, several bad-faith charges, and with a product still in preproduction, DEF CON issued a stop work order. Any claims that DEF CON did not pay Entropic Engineering for its hardware or firmware development are false. Unfortunately, we heard that these issues with Entropic Engineering were not unique to DEF CON. We decided at that point to finish the badge on our own. We paid to send engineers to Vietnam to work onsite to finalize and test the badges in order to ensure they would be done on time for the conference. We never removed Entropic Engineering's logo from our badge, it is still on the PCB. However, Entropic was not involved in the design and production of the case, and we removed their logo we had added as a courtesy.

We were happy to still include one of their contractors on the badge panel session. Unfortunately, shortly before the talk was set to take place DEF CON became aware that unauthorized code had been included in the firmware we had paid Entropic Engineering to produce, claiming credit for the whole badge and promoting their coin wallet to solicit money from DEF CON attendees above and beyond what we had negotiated. When asked about the unauthorized code, the engineer said it had been done as a "joke" two months ago and forgot to remove it, and we decided as an organization not to have him on stage while we kept the slides in the talk giving him credit for his work. We communicated the change in advance of the talk, and this individual decided to show up for the panel anyway. He refused to leave, demanding that our security team remove him. Wanting to ensure that the other people involved in creating the badge were able to deliver their presentation, we complied with his wishes and escorted him off the stage, where he was free to continue attending the conference.

Any issues of non-payment are between him and Entropic Engineering, DEF CON fulfilled its financial obligations.

DEF CON Badge Update!

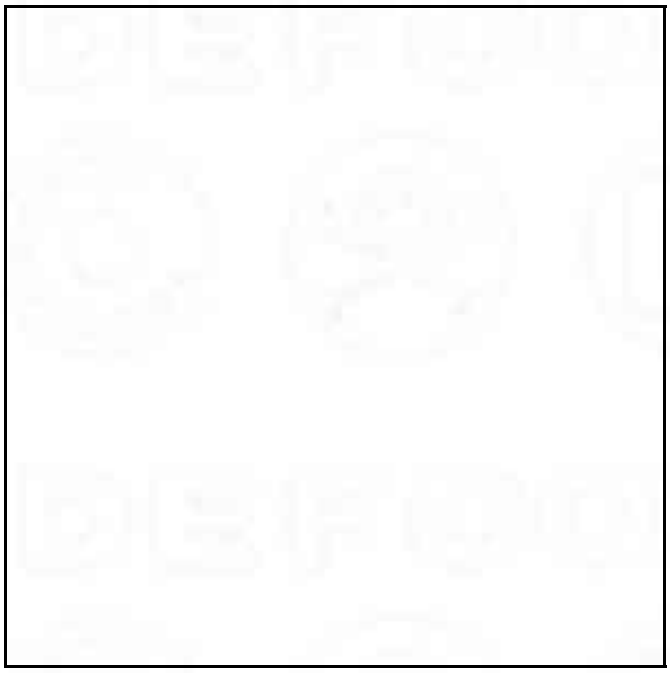
Posted 8.9.24



Thanks to everyone who has reached out to us about the DEF CON 32 badge. We are aware of the save issue and a fix is incoming. Later today we'll have a patch and some instructions for you at defcon.org/badge/32 . We'll keep you posted in these spaces.

DEF CON Hotline!

Posted 8.4.24



You can reach DEF CON staff during normal hours of operation to anonymously report any behavior violating our code of conduct or to find an empathic ear! You can contact us via:

Voice Call, SMS/Text, or Signal: **+1 (725) 222-0934**
or Discord: **@defconhotline**

We hope you have a safe and fun #DefCon32!

Online Registration Closes Soon!

Posted 7.18.24

Just a friendly DEF CON reminder for all our last minute folks - online registration for DEF CON 32 ends August 1. Cash at the door still works, though. Linecon abides.

Pirate Party at DEF CON 32!

Posted 7.2.24

New DEF CON 32 parrrty just dropped! Join us Saturday August 10 for 'Yo Ho Ho, a Pirate's NIght for Me! There'll be a best-dressed pirate contest with a 460 dollar prize and entertainment from O'Craven (Insta: OCRAVEN),NorCal's most swashbuckling Celtic Pirate Rock Band.

For details and updates keep an eye on the DEF CON Music Page . We'll see you there!

Workshops Live! Registration opens soon!

Posted 7.1.24

The wait is over- DEF CON 32's Workshop roster is LIVE! We're quite proud of the lineup! Registration opens at precisely noon Pacific on July 7.

Workshops historically fill up quite quickly so we recommend having a few choices and doing some stretches for maximum click-finger agility.

Good luck to everyone. Just over a month till DC32! Let's GO.

DEF CON Music Presents: Retro Sci-fi Friday Night!

Posted 6.14.24

The good folks at @defcon_music have blessed us with some big party info for #defcon32.

"This year's theme for our Friday Night party is "Retro Sci-Fi"

Be sure to bring your ray guns, Thought immobilizers, Robot sidekicks and of course your best spacesuit!

Sci-Fi costume contest at Midnight!

Winner gets $460 cash!

(Costumes encouraged but not required.)

For more keep an eye on defconmusic.org .

Parties! Meetups! Events! Contests!

Posted 6.12.24

We are enterning the home stretch, citizens of DEF CON! Just under two months until the curtains open - have you prepared yourselves?

The full roster of parties, meetups and events is live on defcon.org to assist in all your various pre-function planning.

Prior Planning Prevents Poor Partying, so get yourself familiarized. While you're there, please make sure to check out the fantastic contest lineup DC32 has ready for you!

It's within sight - just over the horizon. Feel free to get psyched.

See you soon!

Save yourself! Book at The RIO!

Posted 5.22.24

DEF CON 32 #protip: On the desert planet of Las Vegas, door to door AC is worth its weight in water.

When choosing a hotel, don’t overlook our deeply discounted room block in the Rio. All our reserved Rio rooms are fully remodeled suites, and there’s a FREE shuttle right to DEF CON’s main entrance. No wasting your precious moisture on the burning sidewalks.

Also, we have it on good authority the the shuttle moves without rhythm so as not to attract the worm.

Check out the Rio room link now!

Congrats to CTF Qualifying teams!

Posted 5.7.24

Thanks to the fine folks at Nautilus Institute the DEF CON 32 CTF quals are in the books - you can read all about it at https://quals.2024.nautilus.institute/ . There's also a veritable feast of JSON dumps for the curious. Congrats to the winners, thank you to everyone who suited up and we'll see you in Las Vegas!

CTF Quals are Coming!

Posted 4.29.24

Attention packet wizards - the DEF CON 32 CTF Quals Begin May 3!

Our friends at the Nautilus Institute have created a fiendish test of skills that lasts a whole weekend, and the winner gets to compete for everlasting glory in the main event at DEF CON 32.

Will your team rise to the challenge?

You can get your hat in the ring by registering at https://quals.2024.nautilus.institute/

Godspeed to every mad genius who answers the call.

Another new room block - The RIO!

Posted 4.22.24

We've secured a block of deeply discounted rooms at the fabulous Rio , with FREE shuttle service to and from the West Hall of the Las Vegas Convention Center! In addition to the door-to-door shuttle service, they're giving us a big break on the room rate AND the Resort Fee. Rio also offers additional discounts for government employees

We love the Rio - it was home base for DEF CONs 19-22 - and you should see it now. It's had a massive multi-year renovation and it's new all over. New all-suites accomodations, new restaurants, new food hall, even a redesigned 5-acre pool complex. It's a whole new experience at a steal of a price.

We expect these to fill quickly, so you should act accordingly and book now!

New Room Block! Resorts World!

Posted 4.6.24

Spring has sprung. That means laughter in the air, flowers everywhere, and DEF CON right around the corner. In the spirit of new growth we've got another discounted room block for DEF CON 32 attendees - this time it's at Resorts World. You can check the selection and book at this link .

Resorts World is the very large, very new hotel-casino complex that sits on the lot once occupied by The Stardust. It sports a location convenient to the LVCC, the very latest in accommodations and (so far as we can tell) no relation to Michael Crichton's WestWorld and FutureWorld.

It’s all happening, people. Just a few more months till the big event. Prepare accordingly.

Fontainebleau Room Block added!

Posted 3.20.24

We’ve secured a discounted block of rooms at the Fontainebleau Hotel , just across the street from our new location in the LVCC West Hall. To get the discount, follow this link and be sure to reserve by July 4. You can also reserve by phone at (833) 702-7272 - tell ‘em the DEF CON Communications Group sent ya.

The DEF CON season approaches. Feel free to get amped.

DEF CON 32 Call for Papers and More!

Posted 2.22.24

DEF CON 32 preparations are well and truly underway. You can tell because the air is thick with call announcements.

The Calls opening today are:
CFP
Workshops

Demo Labs
Policy

As always, don't procrastinate. The chances of your idea getting over the finish line are better when the reviewer has time to communicate with you.

The information about all the open calls is here . We can't wait to see what you're working on.

DEF CON 32 Online Registration is Open!

Posted 2.19.24

DEF CON is primarily a cash-at-the-door kind of conference. LineCon is in our DNA, and we will always honor it. Long may the beach balls fly.

Still, the option to register online has been a benefit to many attendees. We're keeping that method open for all those who need it.

If that's you, good news! From right now until July 5, 2024, you can register for DC32 at shop.defcon.org .

DEF CON 32 Theme!

Posted 2.5.24

Now that we've got the venue stuff sorted out, we're ready to announce the DEF CON 32 theme!

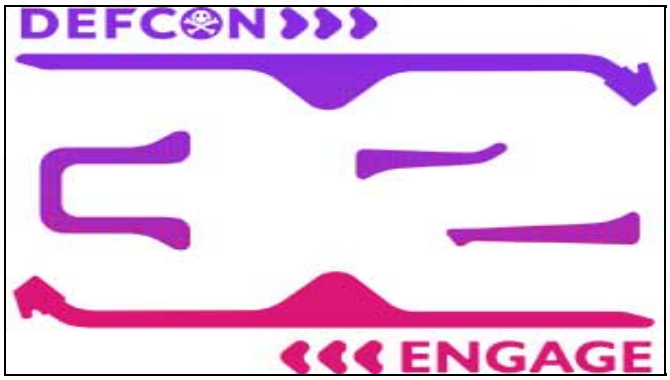
This year's theme is "Engage". The internet may be trending toward a dystopia of dark patterns and walled gardens, but we can do better. We know how. The antidote to apathy and doomscrolling is engagement. You can read The Dark Tangent's full post about it here: https://forum.defcon.org/node/248361 .

The visual vibes are Y2K inspired and you can get your color palette, fonts and whatnot in the DEF CON 32 style guide .

As always, we are excited to see where you'll take this. Let's GO.

We Have Some News About DEF CON 32

Posted 2.4.24



DEF CON was canceled.

After a great 25 year relationship Caesars abruptly terminated their contract with DEF CON, leaving us with no venue for DC 32, and just about seven months to Con!

We don't know why Caesars canceled us, they won't say beyond it being a strategy change and it is not related to anything that DEF CON or our community has done. This kind of no-notice cancellation of a contract is unheard of in the conference business. The parting is confusing, but amicable.

So now we have a challenge. Without a venue, will we be able to UN-Cancel DEF CON 32 before time runs out?

Hackers are flexible. We find solutions. We need a space that can handle an event our size, and configurable enough to accommodate our content. We need a location close to our announced dates, and with super short notice... No small feat.

We immediately scrambled a venue strike team to Las Vegas. Floors were walked. Meetings were held. Hands were shook and options weighed. When the smoke cleared, the field narrowed to one obvious choice and we began forging the requisite agreements.

W00T! DEF CON Is UN-CANCELED!

DEF CON 32 will still be August 8-11 2024, but now held at the Las Vegas Convention Center (LVCC) with workshops and training at the Sahara.

DEF CON 32 will be an adventure where we can try things not possible in our old Casino Hotel spaces. What specifically you ask? Well we are still learning all the specifics but we will have more space, a proper food court, and the largest indoor venue LCD wall in the country.

There are still many questions to be answered, and we have started a live FAQ section on the Forums for DEF CON 32 where we will be updating questions and answers. The initial FAQ is located here: https://forum.defcon.org/node/248358

I look forward to seeing everyone this summer, the start of a new DEF CON era!

-The Dark Tangent

P.S. We made shirts and stickers:
https://shop.defcon.org/products/def-con-un-canceled-mens-t-shirt
https://shop.defcon.org/products/def-con-un-canceled-sticker-set

Big Batch of Calls Open Now for DEF CON 32!

Posted 1.3.24

2024 is officially underway, and we're kicking off DEF CON season with a bunch of of open calls for DC32! Villages, Constests, Parties, Communities - the majority of the calls are open now, with the balance opening February 1. The full list of open calls is available at the Calls Index Page .

Remember, the sooner you get your proposals in, the more chance we can help make your ideas into reality. We can't wait to see what you've got up your sleeves. Happy New Year!

DEF CON Training Las Vegas 2024 is Open for Registration!

Posted 12.15.23

Registration for the DEF CON Training 2024 in Las Vegas is open! Join us August 12-13 right after DEF CON 32 for some two-day, deep-dive technical sessions from some world class trainers. All the details are at training.defcon.org - reserve your spot!

DARPA AIxCC talk from DEF CON 31!

Posted 9.8.23

At DEF CON 31, DARPA announced a huge 2-year AI Cyberchallenge with the semis and finals hosted at good old #defcon. Over 18M in total prizes, access to cutting edge tech and a chance to help secure the open infrastructure we all rely on. If that sounds like your kind of fun, details are at http://aicyberchallenge.com

Throwback Thursday - DEF CON 31 photos!

Posted 8.31.23

More DEF CON 31 goodies going up on the media server: the photos from DC31 are live at media.defcon.org .

Thanks to the DEF CON Photo Corps for all the hard work!

DEF CON 31 Breaking: AI Cyber Challenge Announced for DEF CON 32 & 33

Posted 8.9.23

DEF CON will host the Artificial Intelligence Cyber Challenge #AIxCC semis in 2024 and the final in 2025! @DARPA, @openssf ,@Google, @AnthropicAI @Microsoft & @OpenAI are working together to challenge contestants to create novel AI cybersecurity systems.

Over $18m in cumulative prizes, access to cutting edge tech and a chance to help secure the open infrastructure we all rely on.

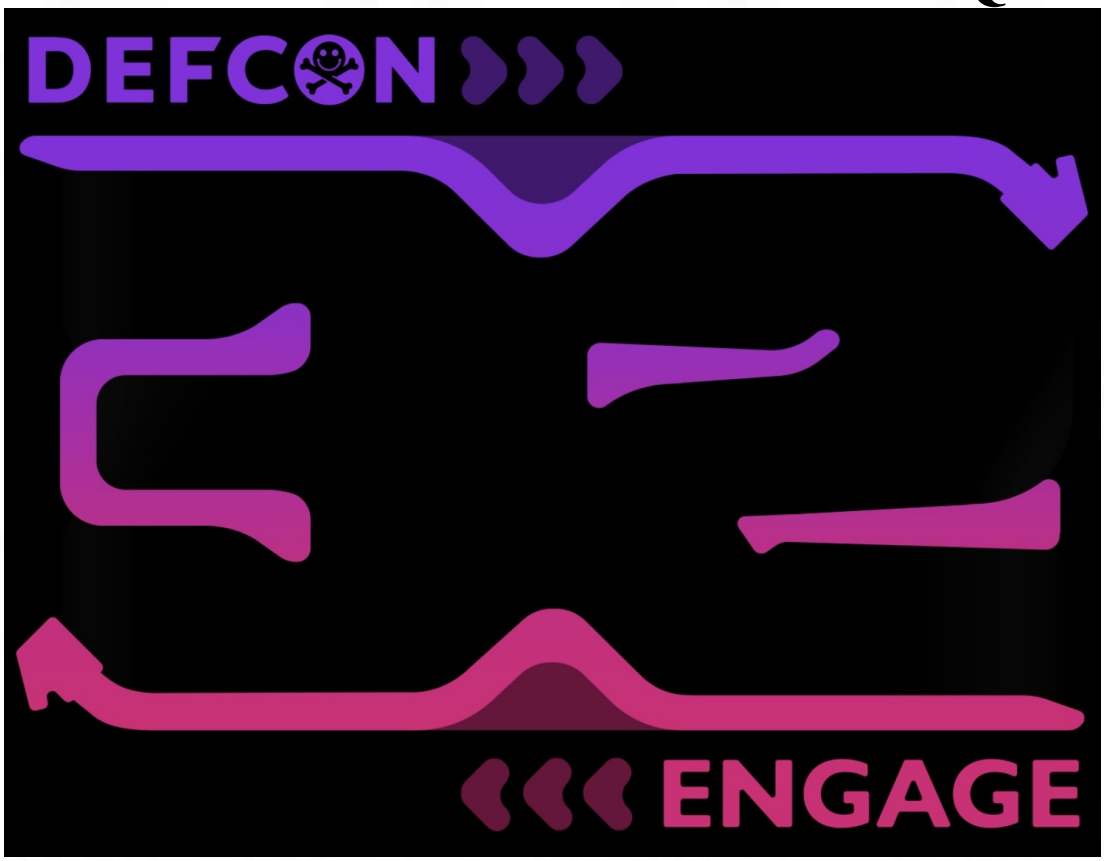
Attend the official announcement at DEF CON 31, Friday at 14:30 in Track 2!

Full details at aicyberchallenge.com

Return to Index

© 1992-2023 DEF CON Communications, Inc. All Rights Reserved | DEF CON Policies | DMCA Information

DEF CON 32 FAQ



This guide will be updated as we learn answers to our questions. If you don’t see an answer to your question please ask and we will do our best to answer.

THE BASICS
When is DEF CON 32?
August 8-11th, 2024

How much will DEF CON 32 badges cost when purchased with cash in-person?
We are still learning about the new venue and hope to announce the price in the coming weeks.

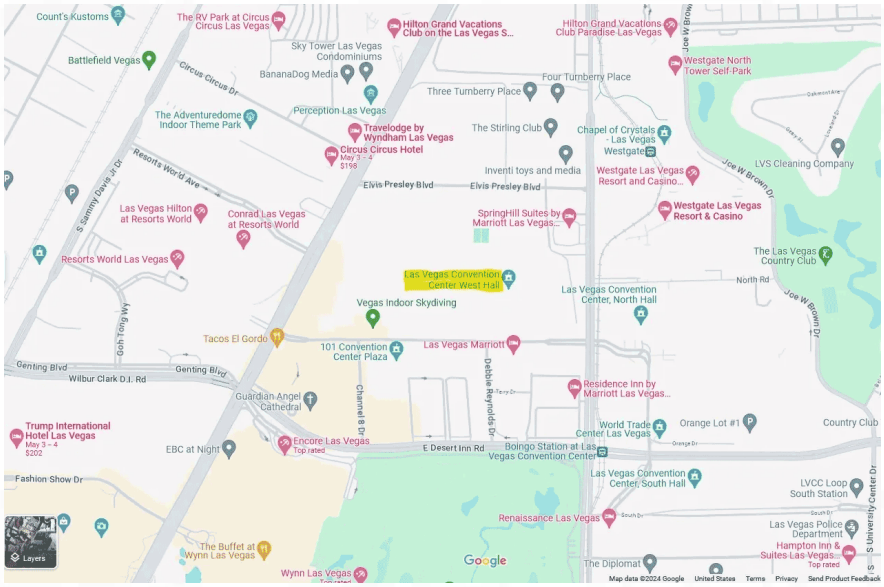
I need to buy a badge online so work will reimburse it.
When badge sales begin they will be available at https://shop.defcon.org/

I need a receipt for the badge, I'm buying with cash.
You will be able to find a DIY receipt on the website, and the media server under DEF CON 32, on August 8th, 2024.

Where is DEF CON 32?
Las Vegas Convention Center (LVCC) West Hall with workshops and training at the Sahara Hotel.
https://en.wikipedia.org/wiki/Las_Ve...vention_Center
https://www.vegasmeansbusiness.com/meeting-facilities/

LVCC West Hall
3150 Paradise Road
Las Vegas, Nevada 89109

Sahara Hotel
https://www.saharalasvegas.com/
2535 Las Vegas Blvd. South
Las Vegas, Nevada 89109



How much space will we have?
A lot. We will have all villages, contests, talks and events under one roof. To give you an idea the LVCC space will be about 800k square feet, and the old Caesars Convention Center was about 550k. Unfortunately a direct sqft comparison is not really the best way to measure space in a convention our size, especially given how complex and unique we are, but you will notice the positive difference.

How will the conference be laid out?
We will know more on floor-plan after we hold a couple on-site planning meetings in February and March. We will update our public maps on the venue page in the coming months, after coordinating with our content creators.

I run a contest / event / village, what does this mean for me?
We have started a separate FAQ for the DEF CON Creators in their planning space.

What are the hours of DEF CON?
Doors open each morning at 08:00 and we go to 02:30 in the morning. On Sunday we shut down after the Closing Ceremonies, around 18:00 (Pacific Time Zone)

DEF CON cash registration and official Merch store will open by 08:00 Thursday the 8th.

What hotels should we stay in?
We have a web page with the hotels we currently have a room block with, and we are working to add more hotels in the coming weeks. Please help us by booking at one of these hotels.
https://defcon.org/html/defcon-32/dc-32-venue.html

What happens if I made a reservation in the Caesars block?
Nothing, you are free to keep it, but you may have further to travel to get to the LVCC.

What is the last day we can cancel our reservations with Caesars Entertainment hotels without an extra fee/fine?
To avoid forfeiture of deposit, please ensure all changes and cancellations are made at least 72 hours prior to scheduled arrival date.

Will new hotels charge a "resort fee" on top of quoted price and taxes? What is being offered to people that sign up under the new DEF CON block at the now hotels?
Each hotel will have separate pricing structures, resort fees, and wifi device limits. As we learn details of our room blocks we will post on the Hotels Page.
https://defcon.org/html/defcon-32/dc-32-venue.html

What about DCTV?
We are currently working the hotel venues to see what is possible, as each hotel has different infrastructure and we are just learning how to work with them. Once we know we will announce and update the hotels page.

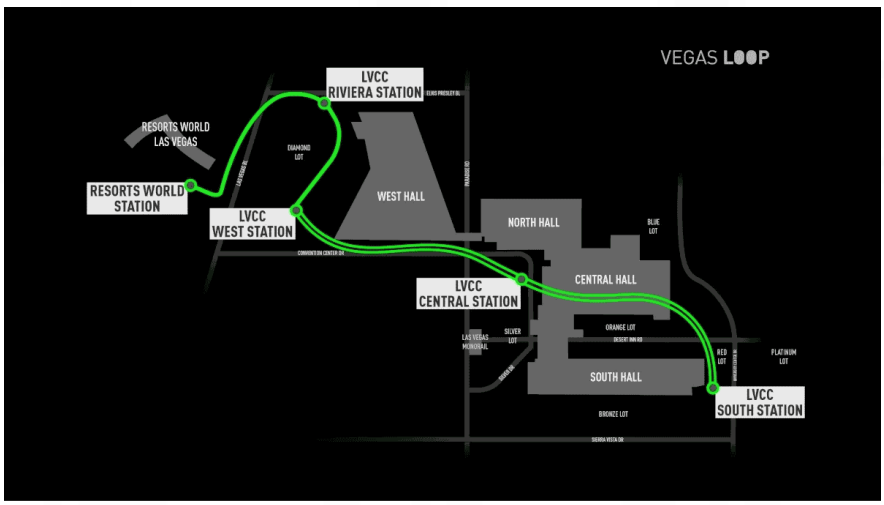
Where can I find a map that shows how we can enter and exit the Las Vegas Convention Center during DEF CON?
We are working to add several maps & directions to the DEF CON website under our Hotel & Venue page.
https://defcon.org/html/defcon-32/dc-32-venue.html

How do I get to the LVCC?
If you are taking a Taxi go to the West Convention Center entrance: 3150 Paradise Road, Las Vegas, Nevada
You can find the current taxi fair at: https://www.lasvegashowto.com/taxi-fare
Currently the taxi cost from the airport to LVCC is speculated at $29.

If you are walking to the LVCC you will enter via the West Convention Center entrance. You can enter by the north lobby or the main atrium entry doors.

Are there any pedestrian bridges over streets to get to the convention center? Where?
Yes, and No. There is a sky bridge crossing paradise road from the north hall to the west hall, but it is really only useful to walk from one end of the LVCC to another.

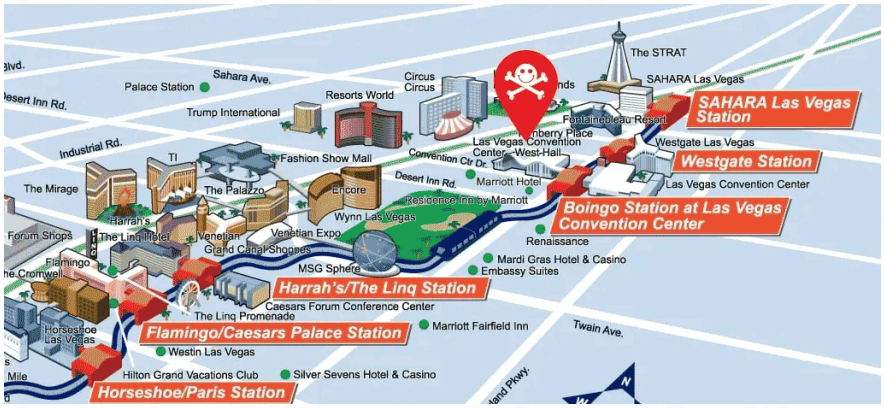
Las Vegas Convention Center Loop.
The Las Vegas Convention Center Loop is an underground transportation system designed to quickly transport passengers throughout the 200-acre Las Vegas Convention Center campus. The system consists of two one-way, .8-mile-long tunnels built to accommodate all-electric Tesla vehicles driving at speeds of up to 35 mph. The LVCC Loop reduces a 25-minute walk to a less than two-minute ride.



Attendees can access the LVCC Loop via three stations:
• West Station – Adjacent to West Hall, this station is located above ground
• Central Station – Near the Central Hall Main Entrance, this station is located below ground and is accessible via escalator or elevator
• South Station – Adjacent to South Hall, this station is located above ground

Las Vegas Monorail

Hours of operation are Mondays, 7 a.m. to midnight; Tuesday through Thursday, 7 a.m. to 2 a.m.; Friday through Sunday, 7 a.m. to 3 a.m.



The Las Vegas Monorail provides a quick and convenient connection along the Las Vegas Strip, linking riders to world-class restaurants, shows, shops, day/nightclubs, spas, hotels and casinos. Directly connected to the Las Vegas Convention Center as well as several resort hotels, the Monorail Is the most convenient way to get around the Strip in Just minutes - without the hassles of traffic or wasted time.

Trains arrive every 4-8 minutes at each of the seven stations: MGM Grand, Bally's/Paris Las Vegas, Flamingo/Caesars Palace, Harrah's, The LINQ, Las Vegas Convention Center, Westgate Resort & Casino, SAHARA Las Vegas.

I'm staying far away. What's the parking situation?
There is parking available, the closest are the diamond and silver lots. When we learn more about our contracted parking arrangement we will publish it on the hotel & venue page.

Will there be any kind of shuttle service from the LVCC to strip hotels?
No

What is the smoking policy at the LVCC?
Smoking is not allowed on the LVCC property, the existing outdoor terraces, or any balconies. Marijuana & tobacco vaping is 100% prohibited, there are uniformed officers with K9 on site trained to smell vaping.

You will have to go outside completely to smoke. Smoking is allowed in the parking lots and sidewalks.

What are the LVCC rules regarding contests/parties/shenanigans?
There will definitely be differences and we expect things to be better for us. We are learning what fees will be to serve alcohol and food.
If you are looking to throw an event, please fill out the call for parties form.
https://defcon.org/html/defcon-32/dc-32-cfopp.html

Can we give away or sell drinks/food/candy at DEF CON?
Please see above. We don't know all the rules yet.

Will DEF CON provide water stations again?
There are water fountains and modern bottle filling stations throughout all 3 floors of the con space. We will include bottle stations on our floor plan map. Remember to bring your bottles!

Since we're going to be in one big non-casino space all day, will there still be Chill-out areas with areas to relax and refuel?
We will have several chill-outs for attendees to sit, rest, hack and or socialize.
The LVCC West Hall has an exclusive food court for our use during the con.
The food hall includes options from: Dunkin' Express, Metro Pizza, Brand Burgers & Fries, Fancy Wok Asian Kitchen, Go Natural, The Roost Farm Fresh Chicken.

Will there be a pool party?
We are securing a pool. If you are interested in throwing a party or a private pool event please contact exhibitors@defcon.org

Will the "Secure DEF CON Wifi Network" work the same way?
The DEF CON NOC will be on the job, and providing secure Wifi.

To learn more about the NOC please visit: https://noc.defcon.org/

HEALTH & PANDEMIC QUESTIONS
What health measures/protocols is DEF CON taking to ensure a safe environment on-site?

DEF CON is working closely with the venue to provide a safe and healthy experience for all. We will comply with whatever safety measures are required of us.

How's the air turnover in the LVCC?
From the LVCC: "The LVCC air filters have a quality rating of MERV 13 and they've increased replacement rate of air filters. The LVCC is also among the first convention centers in the nation to pursue the prestigious GBAC Star Accreditation Program, an accreditation that establishes gold standard cleaning, disinfection and infectious disease prevention protocols that meet or exceed the industry's highest standards of cleanliness for pathogens like the novel coronavirus."

What is your mask policy?
We will have masks on hand for anyone who needs them as well as a finite number of test kits onsite as well. There will be lists of resources for testing and treatment available in the program and at the Info Booth.Wearing a mask remains the safest option, but with these changes our policy is masks strongly recommended.

What will room capacity be?
Room capacity is always set to be capped at fire code standard capacity. In case of changing health and safety recommendations, limits will be reviewed and revised at the direction of Southern Nevada Health District (SNHD).

What's the Lost and Found policy at DEF CON?
If someone comes looking for a lost item, dispatch is radio'd to inquire if it's been reported found. If you can't find an NFO booth, they are marked on the maps in the printed program, website, and the DEF CON Hacker Tracker App. You can call DEF CON 's lost and found at 1-725-377-5045.

LVCC Lost and Found: Central Lobby and West Lobby Security Office. Phone: 702-943-3532 Dispatch closes at the start of DEF CON Closing Ceremonies on Sunday August 11th and all lost items that have not been collected are turned over to the LVCC.

Will you have working elevators and escalators this time?
Yes, the LVCC has several banks of elevators and escalators. The Sahara has replaced all of it's elevators as well, everything is shiny and new.

Do you have ADA or HDA Information?
The DEF CON 32 HDA Guide will be published at the link below when the team receives new information.
https://defcon.org/html/links/dc-hda.html

All hotels are ADA accessible and have staff available to assist attendees before and during the convention. Registered service animals are welcomed by all hotels, and relief areas are provided. These areas are marked on the HDA maps. If you require assistance with hotel issues you may contact any DEF CON Goon, the DEF CON information desk, or the appropriate point of contact for the hotel.

Where can I find general ADA assistance for the Las Vegas Convention Center?
Las Vegas Convention and Visitors Authority
ADA Coordinator
702-892-0711
Nevada Relay Service
Voice: 1-800-326-6888 or Dial 711
TTY/ASCII/HCO: 1-800-326-6868 or Dial 711

Follow the link for the LVCC Guide for visitors with special needs.
https://www.vegasmeansbusiness.com/p...eeds-visitors/

Where can I find interpretation services?
Should you require audio, video or personal interpretation services please contact American Language at 1-800-951-5020

Do you have a plan in case of evacuation?
Customer safety staff at the LVCC is trained to handle emergency situations, they are operational 24 hours a day and become the communications center and command post in the event of an emergency. DEF CON will be working closely with the LVCC customer safety staff for to strategize an emergency action plan. We will update the venue page with emergency exit information as it becomes available.

Will any of the "Call For Everything" deadlines be changes as a result of the new venue?
Calls for Papers, Workshops, Demo Labs, and Policy talks were postponed and expected to launch February 15 2024.
https://defcon.org/html/defcon-32/dc-32-cfi.html

Will any deadlines change for content creators?
No deadlines are set to change.

What's the theme for DEF CON 32?
Our official theme is here: https://defcon.org/html/defcon-32/dc-32-theme.html

---

Return to Index

© 1992-2024 DEF CON Communications, Inc. All Rights Reserved | DEF CON Policies | DMCA Information

DEF CON FAQ

Frequently asked questions about DEF CON

What is DEF CON?

DEF CON is one of the oldest continuously running hacker conventions around, and also one of the largest.

How did DEF CON start?

Originally started in 1993, it was a meant to be a party for member of "Platinum Net", a Fido protocol based hacking network out of Canada. As the main U.S. hub I was helping the Platinum Net organizer (I forget his name) plan a closing party for all the member BBS systems and their users. He was going to shut down the network when his dad took a new job and had to move away. We talking about where we might hold it, when all of a sudden he left early and disappeared. I was just planning a party for a network that was shut down, except for my U.S. nodes. I decided what the hell, I'll invite the members of all the other networks my BBS (A Dark Tangent System) system was a part of including Cyber Crime International (CCI), Hit Net, Tired of Protection (ToP), and like 8 others I can't remember. Why not invite everyone on #hack? Good idea!

Where did the name come from?

The short answer is a combination of places. There as a SummerCon in the summer, a HoHoCon in the winter, a PumpCon during Halloween, etc. I didn't want any association with a time of year. If you are a Phreak, or just use your phone a lot you'll notes "DEF" is #3 on the phone. If you are into military lingo DEF CON is short for "Defense Condition." Now being a fan of the movie War Games I took note that the main character, David Lightman, lived in Seattle, as I do, and chose to nuke Las Vegas with W.O.P.R. when given the chance. Well I knew I was doing a con in Vegas, so it all just sort of worked out.

There are several resources that will give you an idea of what DEF CON is all about.

DEF CON Press: through the prism of the media
DEF CON Groups: Local groups that meet
DEF CON Media Server: DC 1 to the present, captured
Google: always a good research starting point
Just remember, DEF CON is what you make of it.

When and where is DEF CON?

DEF CON is generally in the last week of July or first week of August in Las Vegas. DEF CON 32 will be held August 8th through August 11th, 2024. Many people arrive a day early, and many stay a day later.

Isn't there a DEF CON FAQ already?

Yes, an unofficial one. It's quite humorous, sometimes informative, and DEF CON takes no responsibility for its content. It is archived here.

What are the rules of DEF CON?

Physical violence is prohibited. Harassment of any kind is prohibited. We don't support illegal drug use. Minors should be accompanied by their parent(s) or guardian(s). Please refrain from doing anything that might jeopardize the conference or attendees such as lighting your hair on fire or throwing lit road flares in elevators. DEF CON Goons are there to answer your questions and keep everything moving. Hotel security is there to watch over their property. Each has a different mission, and it is wise to not anger the hotel people. Please be aware that if you engage in illegal activities there is a large contingency of feds that attend DEF CON. Talking about how you are going to bomb the RNC convention in front of an FBI agent is a Career Limiting Move!

You can view the DEF CON Code of Conduct at https://defcon.org/html/links/dc-code-of-conduct.html.

Is DEF CON cancelled?

No.

What is there to do at DEF CON?

DEF CON is a unique experience for each con-goer. If you google around you'll find dozens of write-ups that will give you an idea of what people have experienced at DEF CON. Trust write-ups more than media articles about the con. Some people play capture the flag 24x7, while many people never touch a computer at DEF CON. Some people see every speech they can, while others miss all speeches. Other activities include contests, movie marathons, scavenger hunts, sleep deprivation, lock picking, warez trading, drunken parties, spot the fed contest, the official music events. Because DEF CON is what the attendees make of it, there are more events than even we are aware of. Half the fun is learning what happened at DEF CON after the fact!

I'm not a hacker, should I go to DEF CON?

Many people have different definitions of what is a ‘hacker’. I would recommend looking at previous years speeches, and write-ups from past attendees - this should give you a good idea if DEF CON is for you. This hacker FAQ might give you some insight into the matter as well. If you do not have any technical interests, DEF CON is probably not for you. Sure there is a lot of socializing you can do, but technology and hacking is the core of the con.

Do criminals go to DEF CON?

Yes. They also go to high school, college, work in your workplace, and the government. There are also lawyers, law enforcement agents, civil libertarians, cryptographers, and hackers in attendance. Ssshhh. Don't tell anyone.

What are Goons?

They are the staff at DEF CON. They have many roles including safety, speaker coordination, vendor room coordination, network operations, et cetera... Please try to be helpful to them if they make requests of you. If any goon tells you to move, please do so immediately as there may be safety issues they are attempting to address.

How can I help out or become a Goon?

The staff at DEF CON has grown organically. All positions have some degree of trust associated with them, so typically new goons are ‘inducted’ by friends of existing goons. There are many random points when goons need help and may ask people for help, generally for helping move stuff or other tasks that don't require high amounts of trust or unsupervised work. Just because you help out doesn't make you a goon. If you really want to be a goon, talk with one and see how much work they actually do (Hint: you may want to enjoy being at DEF CON, not working full-time at it). One year the network group got a new Goon when a networking engineer was needed, and he came to the rescue. The intent behind the goons is not to be elitist, but to have a network of trusted people who can help run the conference - please do not feel upset if you are not chosen to be a goon.

How can I help or participate?

DEF CON is not a spectator sport! Before the con, during, and after there are chances for you to get involved. Before the con you can read about the contests and maybe sign up for one like Capture the Flag. There are artwork contests for shirts and posters. You can practice your lock pick skills, or just get your laptop all locked down and ready to do battle. Organize your .mp3s. Check out the DEF CON Forums to see what other people are up to. If you want to create your own event, you can do that as well - you will not get official space or sanctions, but virtually every official event at DEF CON started out as an unofficial event.

I would love to see XYZ event, how do I make this happen?

Virtually all events at DEF CON were conceived by the attendees. The DEF CON forums are a great place for recruiting help for an event you want to put on, and making sure your efforts aren't being duplicated. If it doesn't require resources from DEF CON (space, namely) you generally don't have to ask anyone’s permission. Most events are unofficial until they've been going on for a couple of years. Please let us know if you have an idea for an event, we may help facilitate or promote it. Email [suggestions at DEF CON dot org] to keep us in the loop.

How can I speak at DEF CON?

You can submit a response to our CFP (opening soon). All entries are read and evaluated by a selection committee. We would love to have your submission. The call for papers usually opens in January and closes mid-May.

I'm press, how do I sign up, why can't I get in for free (I'm just doing my job)?

Please email press[at]defcon[d0t]org if you wish press credentials. Lots of people come to DEF CON and are doing their job; security professionals, federal agents, and the press. It wouldn't be fair to DEF CON attendees if we exempted one group from paying. If you are a major network and plan on doing a two minute piece showing all the people with blue hair, you probably shouldn't bother applying for a press pass - you won't get one. If you are a security writer or from a real publication please submit, and someone will respond with an answer.

I want to sell stuff, how do I do this?

If you want a space in our vendor area, you need to apply. Because of limited space and our attempt to have a diversity of vendors, you may not be able to get a booth. It is wise to think of staffing issues - if you are one person do you want to spend your entire time behind a vendors booth?

What are the different price rates?

Everyone pays the same: The government, the media, the ‘well known hackers’, the unknown script kiddies. The only discount is for Goons and speakers, who get to work without paying for the privilege.

How much is admission DEF CON, and do you take credit cards?

The price for DEF CON 32 is $460 USD cash at the door. We do this for a number of reasons. Paying in cash protects your privacy and we can’t be forced to hand over records we don’t collect. Still, offering online registration for DEF CON Safe Mode taught us we had some attendees who really benefit from the option for things like group orders and expense report requirements.

For those attendees who need a credit card option we’ll continue to offer online ticket sales for $480 USD at shop.defcon.org. We hope this makes things easier for the community members who need it.

Does my underage child need a badge?

Children under the age of 8 will not need to purchase a badge.

Can I get a discount on DEF CON badges?

DEF CON charges one price regardless of your social status or affiliation. Please know that we depend on attendee income to pay the costs of the conference and don't have sponsors to help defray the expenses.

We sometimes get requests for discounts [students, veterans, children], unfortunately we don't want to try and validate if you are a current student, look at your ID to determine your age, decode military discharge papers, etc.

If you really want to attend DEF CON for free then do something for the con.

You could:
Submit a CFP and be an accepted speaker or workshop instructor.
Work on a contest, event, or village.
Qualify for CTF/Contests that include entry.
Find a team to become a Goon newbie.
Contribute to content, or perform some entertainment.

I need a letter of invite for my visa application, how do I get that?

In most cases, DEF CON can send a signed letter of invite, usually within a few short business days once we have all the info. If you also require verification of housing, we can put you in touch with someone to help you get your hotel stay organized, let

us know if you need that.

Along with your request, please email us the following to info(at)defcon(.)org

Name as is on passport:
Passport number:
Country of issue:
Date of issue:
Date of expiration:
Country of origin:

DEF CON is too expensive, how can I afford it?

Many people have made an art and science out of coming to DEF CON very cheaply. Here are a couple of tips.

Travel: Buy airfare in advance, go Greyhound, Carpool, hitch-hike. (Note: this may be dangerous and/or illegal.)
Lodging: Share rooms - some people have up to 10 people they share a room with, find a hotel cheaper than the one that the conference is scheduled at, stay up for three days, etc. (note: this can be hazardous to your health.)
Food: Pack food for your trip, go off site to find food, eat in your hotel rooms, and look for cheap Vegas food at Casinos. (Look for deals and specials that are trying to get you in the door to gamble.)
Booze: You don't need to drink. Brew your own and bring it. (It's been done.)
Entrance: Admission can be saved, mow some lawns. Try to go to another 4 day event for cheaper than this that offers so much. We have increased the fees slowly over the years, but also the amount and quality of events have increased.

Inevitably people will try to do some math and pretend that DT gets rich each DEF CON - they seem to lack the ability to subtract.

How many people typically attend DEF CON?

There have been roughly 25-28k attendees in the last few (pre-COVID) years of DEF CON. DEF CON 27 had a record showing with approximately 30,000.

Is there a network at DEF CON?

Why yes, DEF CON is FULLY network-enabled. Now that we've perfected the art of a stable hacker con network, we're ascending to a higher level - we're providing you a network that you feel SAFE in using! Since DEF CON 18 we're WPA2 encrypted over-the-air, with a direct trunk out to the Internet. No peer-to-peer, no sniffing, just straight to the net (and internal servers). We'll provide login credentials at Registration. We know the LTE airwaves will be saturated so we're putting our own cred on the line to give you a net that even we would put our own mobile phones on.

If you're feeling frisky, we'll still have the traditional "open" network for you - bring your laptop (we'd recommend a clean OS, fully patched--you know the procedure) because we don't police what happens on that net. Share & enjoy!

What is the age limit?

People have brought children to DEF CON - it is not recommended to do this unless you are going to constantly supervise them. It is generally an ‘adult’ atmosphere (language, booze, et cetera). If you've never been to DEF CON, you may want to refrain from bringing your children (unless they are demanding that you bring them). While there are no age limits, we have

consistently cooperated with parents and/or private investigators who are looking for children that ‘ran away from home’ to go to DEF CON. You will have to be 21 to reserve a room.

What is a DEF CON "Black Badge"?

The Black Badge is the highest award DEF CON gives to contest winners of certain events. CTF winners sometimes earn these, as well as Hacker Jeopardy winners. The contests that are awarded Black Badges vary from year to year, and a Black Badge allows free entrance to DEF CON for life, potentially a value of thousands of dollars.

How can I get a hold of DT? I tried to mail him and haven't seen a response yet.

DT doesn't dislike you, isn't trying to hurt your feelings, and bears you no ill will. The fact is he gets an unmanageable load of mail continually. Mailing him again may elicit a response. Try mailing FAQ (at) DEFCON.ORG if you have a general question that isn't answered here or in the forums.

Is it hot in Vegas?

Yes. Bring sunscreen (high SPF), do not fall asleep near the pool (lest you wake up to sunburn), and do not walk far in the sun unless you are experienced in dealing with extreme heat. The sun is dangerous in Las Vegas. Sleeping in lawn chairs is a sure way to wake up to severe burns in the morning when that bright yellow thing scorches your skin. Drink plenty of water and liquids - remember that alcohol will dehydrate you.

What should I bring?

It depends on what you're going to do at DEF CON. This is discussed in quite some depth on the unofficial DC FAQ, as well as a thread in the DC Forums. You may want to bring fancy (or outrageously silly) clothes for the official Music events, on Friday and Saturday nights, where everyone shows off nifty attire.

How much do rooms cost, and how do I reserve a room?

The DEF CON 32 group room registration is evolving! We are working on room blocks at several hotels.

Currently we have a block at Sahara: https://book.passkey.com/e/50769948

Check the the DEF CON 32 venue page periodically for more as we add them

---

How much is internet access?

We are looking into this. Free (and possibly more dangerous) internet access is available in the convention area.

Will the hotels broadcast the speeches on their cable system?

DEF CON TV has succcessfully streamed all tracks to all the hotels in the past, and a couple of tracks out to the internet, for several years now. We are navigating a new venue and new hotels, so stay tuned. If we can, we probably will!

Will we have DEF CON branded poker chips?

You will have to attend DEF CON to find out.

Will conference attendees have entire floors of hotel rooms to themselves?

Probably not. Hotels have been very cooperative in attempting to centralize the DEF CON attendees, for their convenience and ours, but there will be non-DEF CON attendees in hotel rooms next to us.

This FAQ didn't answer my questions, or was unclear, how can I get further information?

Check out the DEF CON Forums to ask follow up questions.

Return to Index

© 1992-2023 DEF CON Communications, Inc. All Rights Reserved | DEF CON Policies | DMCA Information

Villages Table

Each Village, as it's name may imply, specializes in a topic or aspect of security or computers.

One Page All Villages list with descriptions

DEF CON 32 All Villages Forum page

You may need to scroll to the right to see all info

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
Adversary Village	Map	Sched	Forum	TW @AdversaryVillag https://defcon.social/@AdversaryVillage YT https://youtube.com/AdversaryVillage DC http://adversaryvillage.org/discord TI @AdversaryVillage FB @AdversaryVillage LI @adversaryvillage
Aerospace Village	Map	Sched	Forum	TW @secureaerospace LI @aerospace-village TW @hack_a_sat DC https://discord.gg/gV4EWuk YT https://www.youtube.com/c/AerospaceVillage https://defcon.social/@aerospacevillage
AppSec Village	Map	Sched	Forum	TW @AppSec_Village LI @appsecvillage YT https://www.youtube.com/c/AppSecVillage DC https://discord.gg/5XY8qYXd7R
Artificial Intelligence Village	Map	Sched	Forum	TW @aivillage_dc TI @aivillage YT link DC https://discord.com/invite/GX5fhfT
Artificial Intelligence Cyber Challenge	Map	Sched	Forum	TW @DARPA
Bio Hacking Village	Map	Sched	Forum	TW @dc_bhv LI @biohacking-village YT http://youtube.com/biohackingvillage TI @biohackingvillage DC https://discord.gg/Q8ubDb5 IG @biohacking_village link
Blacks in Cybersecurity	Map	Sched	Forum	TW @BlackInCyberCo1 https://defcon.social/@blacksincyber TI @blacksincybersecurity YT link LI @blackincyberconference PT @blacksincybersecurity FB @blackincyberconf
Blue Team Village	Map	Sched	Forum	TW @BlueTeamVillage TI @blueteamvillage YT https://www.youtube.com/c/blueteamvillage DC https://discord.gg/blueteamvillage

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
				https://defcon.social/@blueteamvillage
Bug Bounty Village	Map	Sched	Forum	TW @BugBountyDEFCON YT https://www.youtube.com/BountyTalks TW @arl_rose TW @infinitelogins YT https://www.youtube.com/infinitelogins
Car Hacking Village	Map	Sched	Forum	TW @CarHackVillage YT http://youtube.com/@carhackingvillage LI @car-hacking-village DC https://discord.gg/JWCcTAM
Cloud Village	Map	Sched	Forum	TW @cloudvillage_dc YT https://www.youtube.com/cloudvillage_dc DC https://discord.gg/EygUDJABee
Contests	Map	Sched	Forum	link
Crypto Privacy Village	Map	Sched	Forum	TW @cryptovillage SL https://cryptovillage.slack.com/ YT link TI @cryptovillage https://defcon.social/@cryptovillage
Data Duplication Village	Map	Sched	Forum	TW @DDV_DC
DEF CON DemoLabs	Map	Sched		
DEF CON Groups	Map			
DEF CON Groups VR	Map	Sched		TW @DCGVR TI @defcon_groups DC https://discord.gg/bsX4QXf3rD YT link
DEF CON Hackers with Disabilities	Map			TW @HDA_DEFCON
DEF CON Talks	Map	Sched		TW @defcon FB @defcon YT https://www.youtube.com/user/DEFCONConference http://www.reddit.com/r/defcon IG @wearedefcon DC https://discord.gg/defcon
DEF CON Workshops	Map	Sched		
Embedded Systems Village	Map		Forum	TW @EmbeddedVillage
Ham Radio Village	Map	Sched	Forum	TW @HamRadioVillage TI @HamRadioVillage DC https://discord.gg/hrv https://defcon.social/@HamRadioVillage
Hardware Hacking Solder Skills Villages	Map	Sched	Forum	TW @DC_HHV https://defcon.social/@DC_HHV
Industrial Control Systems Village	Map	Sched	Forum	TW @ICS_Village LI @icsvillage YT link TI @ics_village
Internet Of Things Village	Map	Sched	Forum	TW @iotvillage TW @ISEsecurity TW @Villageidiotlab

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
				https://defcon.social/@IoTVillage/ TI @iotvillage YT https://www.youtube.com/c/IoTVillage/videos DC https://discord.gg/EFKbNFrFaN
Lock Pick Village	Map	Sched	Forum	TW @toool TI @toool_us YT https://youtube.com/c/TOOOL-US https://techhub.social/@TOOOL
Misc		Sched		
Packet Hacking Village	Map	Sched	Forum	TW @wallofsheep FB @wallofsheep YT https://youtube.com/wallofsheep TI @wallofsheep PS https://www.periscope.tv/wallofsheep https://defcon.social/@wallofsheep IG @wallofsheep
Password Village	Map			TW @PasswordVillage TI @passwordvillage YT link
Payment Village	Map	Sched	Forum	TW @paymentvillage TI @paymentvillage YT link https://t.me/paymentvillage
Physical Security Village	Map		Forum	TW @physsec TI @bypassvillage LI @physsec https://defcon.social/@physsec
Policy Village	Map		Forum	TW @DEFCONPolicy link https://defcon.social/@defconpolicy
Quantum Village	Map		Forum	TW @quantum_village DC https://discord.gg/6WUjH5cBXu LI @quantumvillage YT https://youtube.com/@quantum_village/
Radio Frequency Village	Map		Forum	TW @rfhackers TW @rf_ctf link DC https://discordapp.com/invite/JjPQhKy
Recon Village	Map	Sched	Forum	TW @ReconVillage FB @reconvillage YT https://www.youtube.com/reconvillage/
Red Team Village	Map	Sched	Forum	TW @RedTeamVillage_ YT https://www.youtube.com/redteamvillage TI @redteamvillage DC https://discord.gg/redteamvillage
Social Activities: Parties/Meetups			Forum	
Social Engineering Village	Map	Sched	Forum	TW @sec_defcon YT link TI @se_community

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
				LI @social-engineering-community FB @Social-Engineering-Community-108883855139272
Tamper Evident Village	Map		Forum	
Telecom Village	Map	Sched	Forum	TW @TelecomVillage
Voting Village	Map		Forum	TW @votingvillagedc YT link TI @votingvillagedc LI @election-integrity-foundation IG @votingvillage?igsh=MWJreTh6dGl3eDEzNg==
XR Village	Map		Forum	TW @XRVillage LI @xr-village https://defcon.social/@xrvillage

Contests Table

Various contests, some lasting all 4 days of DEF CON, some short time on stage

The Contests will be in LVCC West, Hall 4

One Page All Contests list with descriptions

DEF CON 32 All Contests Forum page

You may need to scroll to the right to see all info

? Cube Contest Info	[CANCELED] AutoDriving CTF Contest Info
[Canceled] Resilience Contests Contest Info	5N4CK3Y Contest Info
A Wall of Bribes Contest Info	Adversary Wars CTF Contest Info
AI Art Battle Contest Info	Aw, man pages Contest Info
Betting on Your Digital Rights: 3rd Annual EFF Benefit Poker Tournament at DEF CON 32 Contest Info	Beverage Chilling Contraption Contest Contest Info
Biohacking Village CTF Contest Info	Blacks in Cyber CTF Contest Info
Blue Team Village CTF Contest Info	Capture the Packet Contest Info
Car Hacking Village CTF Contest Info	Chasse Partie Systems CTF Contest Info
Cloud Village CTF Contest Info	CMD+CTRL at DEF CON 32 Contest Info
CrackMeIfYouCan Contest Info	Crash and Compile Contest Info
Creative Writing Short Story Contest Contest Info	Cyber Defender – The Game Contest Info
Darknet-NG Contest Info	DARPA's Artificial Intelligence Cyber Challenge (AIxCC) Contest Info
DC Kubernetes Capture the Flag (CTF) Contest Info	DC Sticker Design Contest Contest Info
DC's Next Top Threat Model (DCNTTM) Contest Info	DEF CON 32 Beard and Mustache Contest Contest Info
DEF CON MUD Contest Info	DEF CON Scavenger Hunt Contest Info
Embedded CTF Contest Info	Feet Feud (Hacker Family Feud) Contest Info
Gold Bug Challenge Contest Info	Hac-Man Contest Info
Hack3r Runw@y Contest Info	Hacker Cooling Contraption Challenge, brought to you by the TeleChallenge

	Contest Info
Hacker Jeopardy Contest Info	HackFortress Contest Info
Hacking Boundary Terminal Contest Info	Ham Radio Fox Hunt Contest Info
Hardware Hacking Village CTF Contest Info	HardWired Contest Info
HTB CTF: Data Dystopia Contest Info	ICS CTF Contest Info
IoT Village CTF Contest Info	It's In That Place Where I Put That Thing That Time Contest Info
Live Recon Contest Contest Info	Lonely Hard Drive Contest Info
Lonely Tag Contest Info	Malware Contests: MARC I & BOMBE Contest Info
Octopus Game Contest Info	Phish Stories Contest Info
PhreakMe presented by HackedExistence Contest Info	Pinball High Score Contest Contest Info
Pub Quiz Contest Info	QOLOSSUS Contest Info
Radio Frequency Capture the Flag Contest Info	REALI7Y OVERRUN Contest Info
Red Alert ICS CTF Contest Info	Red Team Village CTF Contest Info
SEC Vishing Competition Contest Info	Social Engineering Community (SEC) Youth Challenge Contest Info
spyVspy Contest Info	Tinfoil Hat Contest Contest Info
venator aurum – A Treasure Hunt Contest Info	Whose Slide Is It Anyway? Contest Info

DemoLabs Table

Brief demonstrations for people to show off their project.

The DemoLabs are in rooms at LVCC West, Level 3

One Page All Demolabs list with descriptions

DEF CON 32 All Demolabs Forum page

You may need to scroll to the right to see all info

5Ghoul Framework – 5G NR Attacks & 5G OTA Fuzzing Demolabs Info
Automated Control Validation with Tommyknocker Demolabs Info
Bluetooth Landscape Exploration & Enumeration Platform (BLEEP) Demolabs Info
BypassIT – Using AutoIT & Similar Tools for Covert Payload Delivery Demolabs Info
Cloud Offensive Breach and Risk Assessment (COBRA) Demolabs Info
CODASM – Hiding Payloads in Plain .text Demolabs Info
Cyber Security Transformation Chef (CSTC) Demolabs Info
distribRuted – Distributed Attack Framework Demolabs Info
Docker Exploitation Framework Demolabs Info
Drop-Pi Demolabs Info
FACTION Demolabs Info
Farming Ndays with GreyNoise Demolabs Info
Garak Demolabs Info
GC2 – The First Serverless Command & Control Demolabs Info
HIDe & SEEK Demolabs Info
Hopper – Distributed Fuzzer Demolabs Info
Maestro Demolabs Info
MITRE Caldera for OT Demolabs Info
MITRE Caldera Demolabs Info

Moriarty Demolabs Info
MPT – Pentest in Action Demolabs Info
Nebula – 3 Years of Kicking *aaS and Taking Usernames Demolabs Info
Open Hardware Design for BusKill Cord Demolabs Info
SCAGoat – Exploiting Damn Vulnerable SCA Application Demolabs Info
Serberus Demolabs Info
Skynet Demolabs Info
Tempest Demolabs Info
Tengu Marauder Demolabs Info
Testbed Virtual Factory Demolabs Info
The Metasploit Framework v6.4 Demolabs Info
The World Wide Paraweb Demolabs Info
TheAllCommander 2.0 Demolabs Info
Volatile Vault – Data Exfiltration in 2024 Demolabs Info
Vovk – Advanced YARA Rule Generator v2.0 Demolabs Info
XenoboxX – Hardware Sandbox Toolkit Demolabs Info
Zip It Up, Sneak It In – Introduction of apkInspector Demolabs Info

Workshops Table

Longer, more detailed, hands on, lasting half a day.
These have limited seating. These will fill up VERY quickly!
All of the workshops are SOLD OUT at this time.

One Page All Workshops list with descriptions

DEF CON 32 All Workshops Forum page

You may need to scroll to the right to see all info

SOLD OUT – Sold Out – 64-bit Intel Assembly Language Programming for Hackers – Sold Out Workshop Info
SOLD OUT – Sold Out – Capture the Flag 101 – Sold Out Workshop Info
SOLD OUT – Sold Out – Crash Course in Physical Access Control Systems – Sold Out Workshop Info
SOLD OUT – Sold Out – Dissecting and Defeating Ransomware's Evasion Tactics – Sold Out Workshop Info
SOLD OUT – Sold Out – Dissecting Malware for Defense – Crafting Custom Yara Rules – Sold Out Workshop Info
SOLD OUT – Sold Out – Dodging the EDR Bullet: A Workshop on Malware Stealth Tactics – Sold Out Workshop Info
SOLD OUT – Sold Out – Email Detection Engineering and Threat Hunting – Sold Out Workshop Info
SOLD OUT – Sold Out – Finding the Needle: An Introduction to Detection Engineering – Sold Out Workshop Info
SOLD OUT – Sold Out – Flipping the Coin: Red and Blue Teaming in Windows Environments (++) – Sold Out Workshop Info
SOLD OUT – Sold Out – From an attacker's lair to your home: A practical journey through the world of Malware – Sold Out Workshop Info
SOLD OUT – Sold Out – Ghidra Analysis & Automation Masterclass – Sold Out Workshop Info
SOLD OUT – Sold Out – Hack the connected plant! – Sold Out Workshop Info
SOLD OUT – Sold Out – Hacking Apps on Salesforce – Sold Out Workshop Info
SOLD OUT – Sold Out – Hacking The Metal: A Spark of Intelligence – Sold Out Workshop Info
SOLD OUT – Sold Out – Hide your kids, turn off your Wi-Fi, they Rogue APing up in here; 201 – Sold Out Workshop Info
SOLD OUT – Sold Out – Industrial Control Systems: how to secure them in practice! – Sold Out Workshop Info
SOLD OUT – Sold Out – Learning to Hack Bluetooth Low Energy with BLE CTF – Sold Out Workshop Info
SOLD OUT – Sold Out – Long Live Empire: A C2 Workshop for Modern Red Teaming – Sold Out Workshop Info
SOLD OUT – Sold Out – Machine Learning for N00bs – Sold Out Workshop Info

SOLD OUT – Sold Out – Master Class: Hands-On Machine Learning to Enhance Malware Analysis, Classification, and Detection – Sold Out Workshop Info
SOLD OUT – Sold Out – Med Team vs Red Team: Intro into Medical Device Hacking – Sold Out Workshop Info
SOLD OUT – Sold Out – Offensive SCCM: Abusing Microsoft's C2 Framework – Sold Out Workshop Info
SOLD OUT – Sold Out – Playing with RFID – Sold Out Workshop Info
SOLD OUT – Sold Out – Sharp Security from All Angles: Mastering Security in .NET Core 8 and Angular 17 Applications – Sold Out Workshop Info
SOLD OUT – Sold Out – Small Choices, Global Repercussions: A Tabletop Exercise about Decision-Making in Healthcare Cybersecurity – Sold Out Workshop Info
SOLD OUT – Sold Out – Supercharge SAST: Semgrep Strategies for Secure Software – Sold Out Workshop Info
SOLD OUT – Sold Out – Tracing The Pain Away – Practical Binary Tracing Techniques For Defeating Modern Malware Protections – Sold Out Workshop Info
SOLD OUT – Sold Out – Traumatic Library Loading : If you want to use it, you have to implement it… – Sold Out Workshop Info
SOLD OUT – Sold Out – Whitebox Web Exploit Development – Sold Out Workshop Info

Paid Training Table

2 day training sessions on the Mon and Tue after DEF CON. There will be an additional cost for these.

One Page All Paid Training list with descriptions

DEF CON 32 All Paid Training Forum page
DEF CON 32 Training Signup Pages

You may need to scroll to the right to see all info

Party,Gather,Event Table

Various Parties, Gatherings, and Events

One Page All Parties, Gatherings, Events list with descriptions

DEF CON 32 All Parties, Gatherings, Events Forum page

You may need to scroll to the right to see all info

A-ISAC Aviation Cybersecurity Challenge Event Info	Activity: API Security 101: Testing and Trivia by Akto.io Event Info
Activity: Capture the Container by Chainguard Event Info	Activity: Hacking Developers' Trust – Faking GitHub Contribution by Checkmarx Event Info
Activity: Spot the Reachable by Backslash Event Info	Activity: Spot the Secrets: Finding Secrets Throughout Your Environments by GitGuardian Event Info
Activity: Test Your AppSec Knowledge by Deepfactor Event Info	Activity: Threat modelling fun session with OWASP Cornucopia Event Info
Activity: Threat modelling fun session with OWASP Cornucopia Event Info	Activity: Vulnerability Hunt – The Snippets Edition Event Info
AI Village Demos Event Info	All content areas generally open Event Info
AMA on Proxmark3 with Iceman Event Info	ARINC 664 CTF Event Info
Ask Me Anything – Daniel Cutberth, Moderated by Sudhanshu Event Info	Ask the EFF Event Info
Austin School For The Driven Event Info	Biohacking Village: Device Lab Event Info
Blue Team Village Closing Ceremonies Event Info	Book Signings Event Info
Bricks in the Air Event Info	C2Society / DC702 Intro to CTFs Event Info
Capitol Technology University (CTU) Event Info	Car Hacking Village Activities Event Info
Cold Calls Event Info	CubeSat Simulator Event Info
CycleOverride DEF CON Bike Ride Event Info	Darkstar Badge Challenge Event Info
DC Book Club Discussion Event Info	DCNextGen Awards and Closing Ceremony Event Info
DDV open and accepting drives for duplication Event Info	DDV starts accepting drives for duplication Event Info
DEF CON Groups – Open for questions and hanging out	DEF CON Movie Night Event Info

Event Info	
Defcon.run Event Info	Defend the Airport CTF Event Info
Detect a Threat Event Info	Dozier Drill Tournament Event Info
Drone Capture the Flag (CTF) Event Info	Drone Flying Experience Event Info
Drone Hacking Activity Event Info	Drone Hacking Choose Your Own Adventure Event Info
Dumb Terminal fun Event Info	EFF Tech Trivia Event Info
Egor's Keyboard Corner Event Info	Firmware Extraction and Analysis Event Info
Fix the Flag Wargame Event Info	Friendship Bracelet Making Event Info
Game Hacking Community Activities & CTF Event Info	Hack My TV Event Info
Hack the Badge (Badge class level 2) (Overflow if Friday is too full) Event Info	Hack the Badge (Badge class level 2) Event Info
Hack-A-Sat Digital Twin Event Info	Hack-A-Sat Quals Challenges Event Info
Ham Radio Exams Event Info	Hands-On Hardware Hacking – From Console to Root, Manipulating and Controlling a Protected System Event Info
Hard Hat Brigade – Community Space Open Event Info	Hard Hat Brigade – Group Photo and People's Choice Award Event Info
Hardware Hacking and Soldering Skills Village Open (HHV-SSV) Event Info	Hardware Hacking GE Appliances Event Info
HDA Chillout w/ Dj Delchi Event Info	HDA Community – Open for Accessibility Questions/Help Event Info
HDA Presents the open Synth Jam Session Event Info	HHV Rube Goldberg Machine Event Info
Human Registration Open Event Info	ICS Village + XR Village Turn the lights on! Event Info
Important Message Event Info	Inside the Toolkit of Elite Embedded Security Experts – Hands-On Workshop: QEMU & GDB for Embedded Systems Analysis Event Info
Interview – CATO Networks, Hosted by Dhruv Shah Event Info	Interview – Daniel Miessler, Hosted by Ankur Event Info
Interview – Mika Devonshire, Hosted by Himanshu Das Event Info	Interview – RedHunt Labs (Kunal), Hosted by Anant Shrivastava Event Info
Interview – Scott Helme, Hosted by Shubham Event Info	Interview – the gumshoo, Hosted by Ram Event Info
Intigriti Hack Shack Event Info	Intro to Circuit Python (Badge class level 1) (Overflow if Friday is too full) Event Info

Intro to Circuit Python (Badge class level 1) Event Info	IoT Security at DEF CON 32 Event Info
IoT Village Hacking Playground Event Info	ISSCON Event Info
Keysight CTF Challenge Event Info	Last chance to pick up drives at the DDV Event Info
LHC Meshtastic Activities and CTF Event Info	LHC's Unofficial Sticker Swap Table Event Info
Linecon Event Info	Living off the Land inside your WiFi : Exploring and Exploiting Access Points and Routers Event Info
Lockpicking Activities Event Info	Lonely Hackers Club Community Room Open Event Info
Lost & Found Event Info	Merch (formerly swag) Area Open — README Event Info
Name the Noob Event Info	Open Events for DCNextGen Event Info
Packet Detective Event Info	Packet Inspector Event Info
Payment Village CTF Event Info	Peer-to-Peer Mentoring and Networking with optional Swag, Pin & Sticker Exchange Event Info
Phisherman's Wharf – Phishing for Beginners Event Info	Physical Security Village Activities Event Info
Play All the Things Event Info	PTP Flight Challenge Event Info
QOLOSSUS CONTEST Q-CTF Finals Event Info	QOLOSSUS: QUANTUM CTF CONTEST: How to get Started on The Quantum Capture The Flag Event Info
Quantum Village Bloch Party! Event Info	Radio Frequency Village Events Event Info
Recon Village GE(O)SINT Challenge Event Info	Resume Reviews Event Info
Retro Repair Event Info	Robo Sumo Event Info
Safe Hacking Event Info	Safecracking Practical Demonstration Event Info
Secure From Scatch Event Info	SECV – Break / Networking Event Info
Selfie with a CubeSat Event Info	Shell On Demand Appliance Machine (S.O.D.A. Machine) (pronounced SODA) Event Info
Show & Tell Event Info	Signals Are Everywhere Event Info
SIV Internet Voting Hacking Challenge Event Info	Small scale LAN party Event Info
Social Engineering Community Village Hours Event Info	Space Grand Challenge Luna Event Info

Space Systems Security CTF – Platform Security Event Info	spacestudio and spacetower challenges Event Info
Tamper Evident Village Activities Event Info	Telecom Tinkerer CTF Event Info
The Unofficial DEF CON Shoot Event Info	ToolMakers Hackathon Event Info
Toxic BBQ Event Info	Vendors and Exhibitors Open Event Info
Welcome / Badge & Swag Pick Up Event Info	WISP Community & Inclusion Room Event Info
WISP Group Photo Event Info	

Vendors Table

Vendors attending DEF CON

One Page All Vendors list with descriptions

The Vendors are in LVCC West, Hall 4

Aaronia/AudioVideo BrandBuilder Vendor Info
Arts and Entertainment Vendor Info
Boardsource Vendor Info
Cigent Technologies Vendor Info
Cryptocurrency Hackers Vendor Info
Cyber Swamploards Vendor Info
Electronic Cat Vendor Info
Electronic Frontier Foundation Vendor Info
Hacker Warehouse Vendor Info
HackerBoxes Vendor Info
Hackers for Charity Vendor Info
Hak5 Vendor Info
Hotwan Vendor Info
Intrepid Controls Systems, Inc. Vendor Info
Keyport Vendor Info
Mar Williams Vendor Info
Miscreants Vendor Info
Netool Vendor Info
No Starch Press Vendor Info
Nuand Vendor Info

Octopwn Vendor Info
Physical Security Village Vendor Info
Salty Security Vendor Info
Scam Stuff Vendor Info
Science & Design Vendor Info
Shadowvex Vendor Info
SLNT Vendor Info
SOK Vendor Info
SPARROWS Lock Picks Vendor Info
The Calyx Institute Vendor Info
The Tor Project Vendor Info
TOOOL Vendor Info
Women in Security and Privacy (WISP) Vendor Info
Xcape Vendor Info

Exhibitors Table

Exhibitors attending DEF CON

One Page All Exhibitors list with descriptions

DEF CON 32 All Exhibitors Forum page

The Exhibitor room is in LVCC West, Level 1, Hall 3

You may need to scroll to the right to see all info

2600 Exhibitor Info
Altered Security Exhibitor Info
Black Hills Information Security Exhibitor Info
Capitol Technology University Exhibitor Info
CISA Exhibitor Info
Hack the Box Exhibitor Info
Intigriti Exhibitor Info
SquareX Exhibitor Info
Try Hack Me Exhibitor Info

Communities Table

A group of people with common interests, but don’t qualify as a Village, is a Community,

One Page All Communities list with descriptions

DEF CON 32 All Communities Forum page

You may need to scroll to the right to see all info

DCNextGen Community Info
DEF CON Groups (DCG) Community Info
DEF CON Groups VR (DCGVR) Community Info
Friends of Bill W Community Info
Game Hacking Community Community Info
Hard Hat Brigade Community Info
HDA Community Community Info
La Villa Community Info
Lonely Hackers Club Community Info
Makers Community Community Info
Retro Club Community Info
VETCON Community Info
Women in Security and Privacy (WISP) Community Info

Links to DEF CON 32 related pages

Links

DEF CON . org Links

DEF CON Main page
DEF CON 32 Home Page
DEF CON Recent News
DEF CON FAQ
DEF CON 32 FAQ
DEF CON 32 Venue
DEF CON 32 Schedule
DEF CON 32 Policy
DEF CON 32 Training Signup
DEF CON CTF Nautilus Institute, Twitter @Nautilus_CTF
DEF CON YouTube channel, prev years talks

DEF CON Forum Calendar
DEF CON 32 Planning Forum page
DEF CON 32 Hackers with Disabilities HDA Infopack

DEF CON 32 Speakers & Presentations Forum page
DEF CON 32 Villages Forum page
DEF CON 32 Contests Forum page
DEF CON 32 Parties & Gatherings & Events Forum page
DEF CON 32 Demolabs Forum page
DEF CON 32 Workshops Forum page - Registration opened on July 5 at Noon PDT! - All Workshops are Sold Out!
DEF CON 32 Paid Training Forum page - These occur the 2 days following DEF CON

Thanks to the InfoBooth crew for providing access to their backend database. <claps> to their hard work!

Combined Schedules of DEF CON, Villages, and everything else DC32

Hacker Tracker - Android and IOS - the official DEF CON schedule app
The ONE! - A consolidated DEFCON 32 schedule in multiple file formats - html, PDF, CSV, ICAL, epub, mobi, Google calendar
info.defcon.org - the official DEF CON InfoBooth site

Other Interesting Links

DEF CON 32 Planning Highlights
Hackers with Disabilities DEF CON 32 HDA Infopack
@defconparties - calendar
defconmusic - Schedule/News from the DC Artists & Entertainment (A&E) Department
DEFCONorg Twitch stream
defconmusic DEF CON Entertainment Twitch stream
defconmusic YouTube channel
DCTV - DEF CON TV: Twitch streams and Hotel TV channels
#badgelife spreadsheet of unofficial badges for DC32
@qumqats Twitter List of Village accounts to assist in watching Village happenings

Other cons during #SummerHackerCamp

Blackhat	T @BlackHatEvents	FB Black Hat Events
BSides Las Vegas	T @BSidesLV	FB @BSidesLV
Queercon	T @Queercon	FB @queercon
The Diana Initiative	T @Dianainitiative	FB @dianainitiative

Guides/Tips/FAQs

The Definitive Guide to DEF CON
DEF CON A&E - Resources - Rough Distances and Maps
DEF CON A&E - Resources - Packing List
Guide to Attending DEF CON 31
How to Survive Def Con 2022
OpSec For DEF CON 30
DCG 201 Hacker Double Summer 2023 Guides
Birds of a Feather-Resources for 2022 Hacker Summer Camp
Lonely Hackers Club - DEF CON n00b guide - reddit thread
The Lost Policymaker's Guide to Hacker Summer Camp
Holon DEF CON 30 Preparation
DEF CON: The Survival Guide
Preparing for "Hacker Summer Camp"

General / previous years
DEF CON for N00bs
JK-47 - BSidesLV & DEFCON Conference Tips
Just another DEF CON guide
HACKER SUMMER CAMP 2018 GUIDE
On Attending DefCon