

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 28.

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. This year I've added a contests list so you see what's happening and their hours
- DEF CON events are emphasized, so BSLV and BH 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
- 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 28!



DEF CON

DEF CON



DEF CON

DEF CON



DEF CON

DEF CON



DEF CON

DEF CON

Index of DEF CON 28 Activities

[Locations Legends and Info](#)

[Schedule - Thursday - Friday - Saturday - Sunday](#)

[Speaker List](#)

[Talk Title List](#)

[Village Talk List](#)

[AEV - AIV - ASV - BCV - BHV - BTVT1 - BTVW1 - BTVW2 - CHV - CLV - CNE - CPV - CRV - DC - DCG - DL - ENT -](#)

[ETV - FSL - HHV - HRV - HTS - ICS - IOT - LBV - LPV - MOV - PAYV - PHVT - PHVW - POV - PWDV - RCV - RGV -](#)

[RTV - SEV - VMV - WLV](#)

[Talk Descriptions](#)

[DEF CON News](#)

[DEF CON 28 FAQ](#)

[DEF CON FAQ](#)

[Links to DEF CON 28 related pages](#)

Locations Legends and Info

AIV = [Artificial Intelligence Village](#)

Location: [#aiv-general-text](#)

ASV = [AppSec Village](#)

Location: [#asv-general-text](#)

AEV = [AeroSpace Village](#)

Location: [#av-lounge-bar-text](#)

BCV = [Blockchain Village](#)

Location: [#bcv-general-text](#)

BHV = [Bio Hacking Village](#)

Location: [#bhv-general-text](#)

BTVT = [Blue Team Village](#) Talks

BTVW = [Blue Team Village](#) Workshops

Location: [#btv-general-text](#)

CHV = [Car Hacking Village](#)

Location: [#chv-welcome-text](#)

CLV = [Cloud Village](#)

Location: [#cloudv-general-text](#)

CNE = [Contests and Events](#)

CPV = [Crypto Privacy Village](#)

Location: [#cpv-general-text](#)

CRV = [Career Hacking Village](#)

Location: [#cahv-general-text](#)

DC = [DEF CON](#) Talks

DCG = DEF CON Groups
Location: [#dcg-stage-voice](#)

DDV = Data Duplication Village
Location: [#ddv-general-text](#)

DL = DEF CON DemoLabs

ENT = Entertainment (Music)

ETV = Ethics Village
Location: [#ev-general-text](#)

FSL = Fireside Lounge
Location: [#fireside-lounge-voice](#)

HHV = Hardware Hacking Village
Location: [#hhv-infobooth-text](#)

HRV = Ham Radio Village
Location: [#ham-general-text](#)

HTS = Hack The Sea
Location: [#htsv-general-text](#)

ICS = Industrial Control Systems Village
Location: [#ics-general-text](#)

IOT = Internet Of Things Village
Location: [#iotv-general-text](#)

LBV = Lock Bypass Village
Location: [#lbpv-social-text](#)

LPV = Lockpicking Village
Location: [#lpv-general-text](#)

MOV = [Monero Village](#)
Location: [#mv-general-text](#)

PHVT = [Packet Hacking Village Talks](#)
PHVW = [Packet Hacking Village Workshops](#)
Wall of Sheep
Location: [#phv-infobooth-text](#)

PAYV = [Payment Village](#)
Location: [#pay-labs-text](#)

PWDV = [Password Village](#)
Location: [#pwdv-general-text](#)

POV = [Policy Village](#)
Location: [#pol-general-text](#)

RCV = [Recon Village](#)
Location: [#rv-general-text](#)

RGV = [Rogue's Village](#)
Location: [#rov-announcements-text](#)

RTV = [Red Team Village](#)
Location: [#rtv-briefings-text](#)

SEV = [Social Engineering Village](#)
Location: [#sev-general-text](#)

Vendors Area
Vendors Discord channel [#vendors](#)

VMV = [Voting Machine Village](#)
Location: [#vmhv-general-text](#)

WLV = [Wireless Village](#)
Location: [#wv-general-text](#)

Talk/Event Schedule

Thursday

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

Thursday - 07:00 PDT

[Return to Index](#) - [Locations Legend](#)

[RTV - \(07:30-07:59 PDT\) - Red Team Village Announcements and Remarks](#) - Joseph Młodzianowski (cedoXx), Omar r

RTV - The Bug Hunter's Methodology - Jason Haddix

BTVT1 - Blue Team Village - Opening Ceremony

DC - (09:30-09:59 PDT) - [Discovering Hidden Properties to Attack Node.js ecosystem](#) - Feng Xiao

RTV - Red Team Village CTF - Prequal -

RTV - (09:15-10:15 PDT) - [Securing AND Pentesting the Great Spaghetti Monster \(k8s\)](#) - Kat Fitzgerald

WLV - [wicked wardriving with gps and glonass](#) - wytshadow

WLV - [Introduction to WiFi Security](#) - Nishant Sharma

WLV - [Wireless Blue Team](#) - Eric Escobar

WLV - [DragonOS - How I kept busy during COVID19](#) - cemaxecuter

WLV - [The Basics Of Breaking BLE v3](#) - FreqyXin

Thursday - 10:00 PDT

[Return to Index](#) - [Locations Legend](#)

[BTVT1](#) - (10:15-10:59 PDT) - [Graylog: An Introduction Into OpenSOC CTF Tools](#) - Lennart Koopmann

[DC](#) - (10:30-10:59 PDT) - [Room for Escape: Scribbling Outside the Lines of Template Security](#) - Alvaro Munoz,Oleksandr Mirosh

[RTV](#) - cont...(09:15-10:15 PDT) - [Securing AND Pentesting the Great Spaghetti Monster \(k8s\)](#) - Kat Fitzgerald

[RTV](#) - (10:30-11:30 PDT) - [Guerrilla Red Team: Decentralize the Adversary](#) - Christopher Cottrell

Thursday - 11:00 PDT

[Return to Index](#) - [Locations Legend](#)

[BTWV1](#) - (11:15-11:59 PDT) - [Kibana: An Introduction Into OpenSOC CTF Tools](#) - TimDotZero

[DC](#) - (11:30-11:59 PDT) - [DNSSECTION: A practical attack on DNSSEC Zone Walking](#) - Hadrien Barral,Rémi Géraud-Stewart

[RTV](#) - cont...(10:30-11:30 PDT) - [Guerrilla Red Team: Decentralize the Adversary](#) - Christopher Cottrell

[RTV](#) - (11:45-12:45 PDT) - [Evil Genius: Why you shouldn't trust that keyboard](#) - Farith Perez,Mauro Cáseres

[Return to Index](#) - [Locations Legend](#)

[BTWW1](#) - (12:15-12:59 PDT) - OpenSOC CTF Tool Demo: Moloch

[DC](#) - (12:30-12:59 PDT) - [Hacking the Hybrid Cloud](#) - Sean Metcalf

[RTV](#) - cont...(11:45-12:45 PDT) - [Evil Genius: Why you shouldn't trust that keyboard](#) - Farith Perez, Mauro Cáseres

[Return to Index](#) - [Locations Legend](#)

[BTW1](#) - (13:15-13:59 PDT) - [Osquery: An Introduction Into OpenSOC CTF Tools](#) - Whitney Champion

[DC](#) - (13:30-13:59 PDT) - [Hacking traffic lights](#) - Rik van Duijn, Wesley Neelen

[HTS](#) - Dockside with the US Coast Guard

[RTV](#) - [Combining notebooks, datasets, and cloud for the ultimate automation factory](#) - Ryan Elkins

[Return to Index](#) - [Locations Legend](#)

[BTW1](#) - (14:15-14:59 PDT) - [Velociraptor: An Introduction Into OpenSOC CTF Tools](#) - Mike Cohen

[DC](#) - (14:30-14:59 PDT) - [Hacking the Supply Chain – The Ripple20 Vulnerabilities Haunt Hundreds of Millions of Critical Devices](#) - Ariel Schön, Moshe Kol, Shlomi Oberman

[RTV](#) - (14:15-15:15 PDT) - [Deep Dive into Adversary Emulation - Ransomware Edition](#) - Jorge Orchilles

[Return to Index](#) - [Locations Legend](#)

[BTW1](#) - (15:15-15:59 PDT) - [Zeek: An Introduction Into OpenSOC CTF Tools](#) - Aaron Soto, Amber Graner

[DC](#) - (15:30-15:59 PDT) - [Demystifying Modern Windows Rootkits](#) - Bill Demirkapi

[RTV](#) - cont...(14:15-15:15 PDT) - [Deep Dive into Adversary Emulation - Ransomware Edition](#) - Jorge Orchilles

[RTV](#) - (15:30-16:30 PDT) - [Introducing DropEngine: A Malleable Payload Creation Framework](#) - Gabriel Ryan

[Return to Index - Locations Legend](#)

[BTW1 - \(16:15-16:59 PDT\) - Suricata: An Introduction Into OpenSOC CTF Tools - Josh](#)

[DC - \(16:30-16:59 PDT\) - Domain Fronting is Dead, Long Live Domain Fronting: Using TLS 1.3 to evade censors, bypass network defenses, and blend in with the noise - Erik Hunstad](#)

[RTV - cont...\(15:30-16:30 PDT\) - Introducing DropEngine: A Malleable Payload Creation Framework - Gabriel Ryan](#)

[RTV - \(16:45-17:45 PDT\) - Zero Trust - A Vision for Securing Cloud and Redefining Security - Vandana Verma Sehgal](#)

[Return to Index - Locations Legend](#)

[BTWV1](#) - (17:15-17:59 PDT) - OpenSOC CTF Tool Demo: Thinkst Canary

[RTV](#) - cont...(16:45-17:45 PDT) - [Zero Trust - A Vision for Securing Cloud and Redefining Security](#) - Vandana Verma Sehgal

[Return to Index - Locations Legend](#)

RTV - What college kids always get wrong, the art of attacking newbies to blueteam - Forrest Fuqua

RTV - (19:15-20:15 PDT) - [Android Malware Adventures](#) - Kürşat Oğuzhan Akıncı, Mert Can Coşkuner

[Return to Index - Locations Legend](#)

RTV - cont...(19:15-20:15 PDT) - [Android Malware Adventures](#) - Kürşat Oğuzhan Akıncı,Mert Can Coşkuner

RTV - (20:30-21:30 PDT) - [Making Breach and Attack Simulation Accessible and Actionable with Infection Monkey](#) - from IT to the C-suite - Shay Nehmad

[Return to Index - Locations Legend](#)

RTV - cont...(20:30-21:30 PDT) - [Making Breach and Attack Simulation Accessible and Actionable with Infection Monkey - from IT to the C-suite](#) - Shay Nehmad

RTV - (21:45-22:45 PDT) - [Android Application Exploitation](#) - Kyle Benac (aka @B3nac)

RTV - cont...(21:45-22:45 PDT) - [Android Application Exploitation](#) - Kyle Benac (aka @B3nac)

[Return to Index - Locations Legend](#)

RTV - Offensive Embedded Exploitation : Getting hands dirty with IOT/Embedded Device Security Testing - Kaustubh Padwad

Friday

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

Friday - 06:00 PDT

[Return to Index - Locations Legend](#)

[CLV - Cloud Village CTF -](#)

[Return to Index - Locations Legend](#)

CLV - cont...(06:00-12:30 PDT) - [Cloud Village CTF](#) -

RTV - (07:30-07:59 PDT) - [Red Team Village Opening Remarks](#) - Joseph Mlodzianowski (cedoXx), Omar r

[Return to Index - Locations Legend](#)

[AEV - Hack-A-Sat Launch Party -](#)

[RTV - Knock knock, who's there? Identifying assets in the cloud - Tanner Barnes \(aka @_StaticFlow_\), NahamSec](#)

Friday - 09:00 PDT

[Return to Index](#) - [Locations Legend](#)

[AIV](#) - (09:30-09:59 PDT) - [Opening Remarks](#) - AI Village Organizers

[BHV](#) - (09:30-10:45 PDT) - [DAY1 KEYNOTE: The Trust Talks](#) - Nina Alli, Vee Schmitt, Yusuf Henriques, Josh O'Connor, Cannibal, Devabhaktuni Srikrishna, Najla Lindsay, Nate DeNicola

[DC](#) - (09:30-09:59 PDT) - [Welcome to DEF CON Safe Mode](#) - The Dark Tangent

[HHV](#) - (09:30-09:59 PDT) - [Meetup: Some HHV Challenges](#) - rehr

[ICS](#) - [Keynote](#) - Chris Krebs

[IOT](#) - (09:15-09:45 PDT) - [How to get rights for hackers](#) - Chloé Messdaghi

[MOV](#) - (09:50-09:59 PDT) - [Welcome Speech](#) - rehr

[PAYV](#) - (09:45-09:59 PDT) - [Welcome to the Payment Village](#) - Leigh-Anne Galloway

[RTV](#) - (09:15-10:15 PDT) - [Red Teaming: Born from the Hacker Community](#) - Chris Wysopal

[RTV](#) - (09:30-15:59 PDT) - [Red Team Village CTF - Finals](#) -

Friday - 10:00 PDT

[Return to Index - Locations Legend](#)

AEV - [Opening Remarks: Getting The Aerospace Village To Take-Off](#) - Chris Krebs,Dr Will Roper,Pete Cooper
AIV - [ML Security Evasion Competition 2020](#) - drhyrum,zh4ck
AIV - (10:30-10:59 PDT) - [Baby's First 100 MLSec Words](#) - erickgalinkin
ASV - [Who's secure, who's not, & who makes that choice](#) - Maddie Stone
BCV - [Welcome Note](#)
BCV - [Key Note - State of Blockchain Security](#) - Peter Kacherginsky
BHV - cont...(09:30-10:45 PDT) - [DAY1 KEYNOTE: The Trust Talks](#) - Nina Alli,Vee Schmitt,Yusuf Henriques,Josh O'Connor,Cannibal,Devabhaktuni Srikrishna,Najla Lindsay,Nate DeNicola
BTVT1 - [Quark Engine - An Obfuscation-Neglect Android Malware Scoring System \(Beginner\)](#) - JunWei Song,KunYu Chen
BTWV1 - [Cypher for Defenders: Leveraging Bloodhound Data Beyond the UI \(Intermediate\)](#) - Scoubi
CHV - [Adding new features by manipulating CAN bus](#) - Teejay
CHV - [Automotive In-Vehicle Networks](#) - Kamel Ghali
CLV - cont...(06:00-12:30 PDT) - [Cloud Village CTF](#) -
CPV - [STARTTLS is Dangerous](#) - Hanno Böck
CRV - [From Barista to Cyber Security Pro, Breaking the Entry Level Barrier](#) - Alyssa Miller
DC - (10:30-10:59 PDT) - [Spectra—New Wireless Escalation Targets](#) - Francesco Gringoli,Jiska Classen
DL - [Carnivore \(Microsoft External Attack Tool\)](#) - Chris Nevin
DL - [CIRCO v2: Cisco Implant Raspberry Controlled Operations](#) - Emilio Couto
ETV - [Federal Communications Commission](#) - Comm. Geoffrey Starks
HHV - [Learn to Solder the BadgeBuddy Kit](#) - Joseph Long (hwbxr)
HRV - [Village Opening Remarks](#) -
HTS - [Yacht PWNed](#) - Stephen Gerling
ICS - (10:15-10:45 PDT) - [ICS Village CTF Kick-Off](#) - Tom
IOT - [IoT Hacking Stories in Real Life](#) - Besim Altinok
IOT - (10:45-11:45 PDT) - [Getting Started – Building an IoT Hardware Hacking Lab](#) -
LBV - [Bypass 101 + Q&A](#)
LPV - [Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
MOV - [Keynote: Monero: Sound Money Safe Mode](#) - Dr. Daniel Kim
PAYV - [Making sense of EMV card data – decoding the TLV format](#) - Dr Steven J. Murdoch
PHVT - [Media Analysis of Disinformation Campaigns](#) - Chet Hosmer,Mike Raggo
PWDV - [Getting Started with Hashcat](#) - Password Village Staff
RTV - cont...(09:15-10:15 PDT) - [Red Teaming: Born from the Hacker Community](#) - Chris Wysopal
RTV - cont...(09:30-15:59 PDT) - [Red Team Village CTF - Finals](#) -
RTV - (10:30-11:30 PDT) - [Panel: The Joy of Coordinating Vulnerability Disclosure](#) - Daniel Gruss,CRob,Lisa Bradley,Katie Noble,Omar Santos, Anders Fogh
VMV - [Welcome and Kick-Off](#) - Harri Hursti,Matt Blaze,Maggie MacAlpine
VMV - (10:30-10:59 PDT) - [Keynote Remarks: Representative Jackie Speier](#) - Jackie Speier

[Return to Index - Locations Legend](#)

[AEV - MITM - The Mystery In The Middle. An Introduction To The Aircraft Information Systems Domain](#) - Matt Gaffney

[AIV - Workshop 1](#)

[ASV - 2FA in 2020 and Beyond](#) - Kelley Robinson

[ASV - Applying Pysa to Identify Python Security Vulnerabilities](#) - Graham Bleaney

[BCV - Verifiable Delay Functions for preventing DDoS Attacks on Ethereum 2.0](#) - Gokul Alex,Tejaswa Rastogi

[BHV - Fireside Chat with Dr. Amy Abernethy and Adama Ibrahim](#) - Adama Ibrahim,Amy Abernethy

[BHV - \(11:30-11:59 PDT\) - Porcupine: Rapid and robust tagging of physical objects using DNA with highly separable nanopore signatures](#) - Katie Doroschak

[BTVT1 - OuterHaven - The EFI Memory Space Just Itching to be Misused \(Intermediate\)](#) - Connor Morley

[BTVW1 - cont...\(10:00-11:30 PDT\) - Cypher for Defenders: Leveraging Bloodhound Data Beyond the UI \(Intermediate\)](#) - Scoubi

[BTVW2 - \(11:30-13:30 PDT\) - An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology \(Beginner\)](#) - Ben Bornholm

[CHV - PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS](#) - Ben Gardiner,Chris Poore

[CHV - OBD and what we CAN do with it](#) - Infenet

[CLV - cont...\(06:00-12:30 PDT\) - Cloud Village CTF](#) -

[CLV - Opening Keynote](#)

[CLV - \(11:20-12:05 PDT\) - IAM Concerned: OAuth Token Hijacking in Google Cloud \(GCP\)](#) - Jenko Hwong

[CPV - LadderLeak: Breaking ECDSA With Less Than One Bit Of Nonce Leakage](#) - Akira Takahashi,F. Novaes,M. Tibouchi,Y. Yarom,Diego F. Aranha

[CRV - But I Still Need A Job!](#) - Kirsten Renner

[DC - \(11:30-11:59 PDT\) - Pwn2Own Qualcomm compute DSP for fun and profit](#) - Slava Makkaveev

[DL - cont...\(10:00-11:50 PDT\) - Carnivore \(Microsoft External Attack Tool\)](#) - Chris Nevin

[DL - cont...\(10:00-11:50 PDT\) - CIRCO v2: Cisco Implant Raspberry Controlled Operations](#) - Emilio Couto

[HHV - Hardware hacking 101: There is plenty of room at the bottom](#) - Federico Lucifredi

[HRV - Ham Radio USA License Exams \(Friday\)](#) -

[HRV - Talking to Satellites](#) -

[ICS - Mission Kill: Process Targeting in ICS Attacks](#) - Joe Slowik

[ICS - \(11:45-12:15 PDT\) - Vulnerability Discovery - Tips for Surviving and Thriving](#) - Dor Yardeni,Mike Lemley

[IOT - cont...\(10:45-11:45 PDT\) - Getting Started – Building an IoT Hardware Hacking Lab](#) -

[LBV - cont...\(10:00-11:30 PDT\) - Bypass 101 + Q&A](#)

[LBV - \(11:30-12:59 PDT\) - DIY Bypass Tool Workshop + Q&A](#)

[LPV - Key Duplication - It's not just for the movies!](#) - Tony Virelli

[MOV - cont...\(10:00-11:30 PDT\) - Keynote: Monero: Sound Money Safe Mode](#) - Dr. Daniel Kim

[PAYV - Fear and Loathing in Payment Bug Bounty](#) - Timur Yunusov

[RGV - Rogues Village Introduction](#) - Rogues Village Team

[RTV - cont...\(09:30-15:59 PDT\) - Red Team Village CTF - Finals](#) -

[RTV - cont...\(10:30-11:30 PDT\) - Panel: The Joy of Coordinating Vulnerability Disclosure](#) - Daniel Gruss,CRob,Lisa Bradley,Katie Noble,Omar Santos, Anders Fogh

[RTV - \(11:45-12:45 PDT\) - How to hack SWIFT, SPID, and SPEI with basic hacking techniques \(from a Red Team Perspective\)](#) - Guillermo Buendia

[VMV - A Policy Approach to Resolving Cybersecurity Problems in the Election Process](#) - Jody Westby

[VMV - \(11:30-12:30 PDT\) - Hacking Democracy II: On Securing an Election Under Times of Uncertainty and Upheaval](#) - Casey John Ellis,Kimber Dowsett,Tod Beardsley,Jack Cable,Amèlie Koran

Friday - 12:00 PDT

[Return to Index - Locations Legend](#)

AEV - [Satellite Orbits 101](#) - Matt Murray
AEV - (12:30-12:59 PDT) - [GPS Spoofing 101](#) - Harshad Sathaye
AIV - cont...(11:00-12:30 PDT) - Workshop 1
ASV - cont...(11:00-12:59 PDT) - [Applying Pysa to Identify Python Security Vulnerabilities](#) - Graham Bleaney
ASV - [Android Bug Foraging](#) - João Morais, Pedro Umbelino
BCV - [Security Focused Operating System Design](#) - Colin Cantrell
BHV - [Redefining patient safety in the digital era](#) - Dena Medelsohn, Jen Goldsack
BTVT1 - (12:30-12:59 PDT) - [No Question: Teamviewer, Police and Consequence \(Beginner\)](#) - corvusactual
BTVW2 - cont...(11:30-13:30 PDT) - [An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology \(Beginner\)](#) - Ben Bornholm
CHV - [Before J1939: A J1708/J1587 Protocol Decoder](#) - Thomas Hayes, Dan Salloum
CHV - [Fundamentals of Diagnostic Requests over CAN Bus](#) - Robert Leale (CarFuCar)
CLV - cont...(06:00-12:30 PDT) - [Cloud Village CTF](#) -
CLV - cont...(11:20-12:05 PDT) - [IAM Concerned: OAuth Token Hijacking in Google Cloud \(GCP\)](#) - Jenko Hwong
CLV - [Ransom in the Cloud](#) - Spencer Gietzen
CLV - (12:50-13:25 PDT) - [Static analysis of Infrastructure as code: Terraform, Kubernetes, Cloudformation and more!](#) - Barak Schoster
CPV - [The Norwegian Blue: A lesson in Privacy Engineering](#) - Eivind Arvesen
CRV - [Hacking Security Leadership](#) - Pete Keenan
DC - (12:30-12:59 PDT) - [Detecting Fake 4G Base Stations in Real Time](#) - Cooper Quintin
DL - [PyRDP: Remote Desktop Protocol Monster-in-the-Middle \(MITM\) and Library](#) - Olivier Bilodeau
DL - [Mobile Security Framework - MobSF](#) - Ajin Abraham
ETV - [U.S. Privacy and Civil Liberties Oversight Board Member](#) - Travis LeBlanc
HHV - (12:30-12:59 PDT) - [onkeypress=hack\(\);](#) - Farith Pérez Sáez, Luis Ángel Ramírez Mendoza (@Iarm182luis), Mauro Cáseres
HRV - cont...(11:00-13:59 PDT) - [Ham Radio USA License Exams \(Friday\)](#) -
HTS - [Build a Raspberry AIS](#) - Dr. Gary Kessler
ICS - cont...(11:45-12:15 PDT) - [Vulnerability Discovery - Tips for Surviving and Thriving](#) - Dor Yardeni, Mike Lemley
ICS - (12:30-13:30 PDT) - [On the insecure nature of turbine control systems in power generation](#) - Alexander Korotin, Radu Motspan
IOT - (12:15-12:59 PDT) - [Exploring vulnerabilities in Smart Sex Toys, the exciting side of IoT research](#) - Denise Giusto Bilic
LBV - cont...(11:30-12:59 PDT) - [DIY Bypass Tool Workshop + Q&A](#)
LPV - [Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
MOV - [Proposed Mitigation Measures to Address a Disruption Such as The Economic Impact of COVID -19 on Transaction Capacity and Fees in Monero](#) - Dr. Francisco "ArticMine" Cabañas
RGV - [Google Maps Hacks](#) - Simon Weckert
RTV - cont...(09:30-15:59 PDT) - [Red Team Village CTF - Finals](#) -
RTV - cont...(11:45-12:45 PDT) - [How to hack SWIFT, SPID, and SPEI with basic hacking techniques \(from a Red Team Perspective\)](#) - Guillermo Buendia
VMV - cont...(11:30-12:30 PDT) - [Hacking Democracy II: On Securing an Election Under Times of Uncertainty and Upheaval](#) - Casey John Ellis, Kimber Dowsett, Tod Beardsley, Jack Cable, Amèlie Koran
VMV - (12:30-12:59 PDT) - [See Something, Say Something](#) - Marten Mickos

[AEV - Building Connections Across The Aviation Ecosystem](#) - Katie Noble,Al Burke,Jeff Troy,Jen Ellis,John Craig,Randy Talley (CISA),Sidd Gejji

[AIV - Hyperlocal Drift detection with Goko: Finding abusers of your Dataset](#) - comathematician

[AIV - \(13:30-13:59 PDT\) - Spectrum: An End-to-End Framework for ML-based Threat Monitoring and Detection](#) - Nahid Farhady

[ASV - Our journey into turning offsec mindset to developer's toolset](#) - Paul Amar,Stanislas Molveau

[BCV - Cryptocurrencies have superusers?](#) - Mark Nesbitt

[BCV - \(13:30-13:59 PDT\) - Double Spending in BSV, is it Possible?](#) - Poming Lee

[BHV - Russian Cyber Threats in The Pandemic Era](#) - Dr. Khatuna Mshvidobadze

[BTVT1 - \(13:30-14:30 PDT\) - Building BLUESPAWN: An Open-Source, Active Defense & EDR Software \(Intermediate\)](#) - Jake Smith,Jack McDowell

[BTWV1 - \(13:30-14:59 PDT\) - Turning Telemetry and Artifacts Into Information \(Intermediate\)](#) - Omenscan

[BTWV2 - cont...\(11:30-13:30 PDT\) - An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology \(Beginner\)](#) - Ben Bornholm

[CHV - Cluster fuzz!](#) - Mintynet

[CLV - cont...\(12:50-13:25 PDT\) - Static analysis of Infrastructure as code: Terraform, Kubernetes, Cloudformation and more!](#) - Barak Schoster

[CLV - \(13:25-14:10 PDT\) - Can't Touch This: Detecting Lateral Movement in Zero-Touch Environments](#) - Phillip Marlow

[CPV - Dos, Donts and How-Tos of crypto building blocks using Java](#) - Mansi Sheth

[CRV - Key Ingredients for the Job Interviews \(Virtual or Face-2-Face\)](#) - Roy Wattanasin

[DC - \(13:30-13:59 PDT\) - When TLS Hacks You](#) - Joshua Maddux

[DL - cont...\(12:00-13:50 PDT\) - PyRDP: Remote Desktop Protocol Monster-in-the-Middle \(MITM\) and Library](#) - Olivier Bilodeau

[DL - cont...\(12:00-13:50 PDT\) - Mobile Security Framework - MobSF](#) - Ajin Abraham

[HHV - \(13:30-14:30 PDT\) - HackerBox 0057 Build Session](#) - Joseph Long (hwbxr)

[HRV - cont...\(11:00-13:59 PDT\) - Ham Radio USA License Exams \(Friday\)](#) -

[HRV - A Basic Ham Station Setup](#) -

[ICS - cont...\(12:30-13:30 PDT\) - On the insecure nature of turbine control systems in power generation](#) - Alexander Korotin,Radu Motspan

[ICS - \(13:45-14:45 PDT\) - The Journey of ICS Project Files - Visibility and Forensics to Exploitation](#) - Nadav Erez

[IOT - \(13:15-13:59 PDT\) - IoT Under the Microscope: Vulnerability Trends in the Supply Chain](#) - Parker Wiksell

[LBV - General Q&A / Drop-in and Chat](#)

[LPV - Hybrid PhySec tools - best of both worlds or just weird?](#) - d1dymu5

[MOV - This year's village badge](#) - Michael Schloh von Bennewitz

[PHVT - Dumpster Fires: 6 Things About IR I Learned by Being a Firefighter](#) - Dr. Catherine Ullman

[PHVW - Intrusion Analysis and Threat Hunting with Open Source Tools](#) - Jack Mott,Jason Williams,Josh Stroschein

[PWDV - Making Targeted Wordlists](#) - Password Village Staff

[RGV - cont...\(12:00-13:59 PDT\) - Google Maps Hacks](#) - Simon Weckert

[RTV - cont...\(09:30-15:59 PDT\) - Red Team Village CTF - Finals](#) -

[RTV - Trust, but Verify: Maintaining Democracy In Spite of](#) - Allie Mellen

[SEV - Live SE Q&A](#) -

[VMV - A Panel with the Feds on Election Security](#) - Bryson Bort,David Imbordino,Brig. Gen. William Hartman,Matthew Masterson,Cynthia Kaiser,Dan Kimmage

- AEV - [Experimental Aviation, Risks And Rewards](#) - Patrick Kiley
- AIV - [Hacking with Skynet - How AI is Empowering Adversaries](#) - GTKlondike
- BCV - [Creating a decentralized storage for Kubernetes with Tardigrade and Velero](#) - Kevin Leffew
- BHV - [Digital Health Technologies in the NIH All of Us Research Program](#) - Michelle Holko
- BHV - (14:30-15:30 PDT) - [Medical Device Vulnerability Disclosure](#) - Chloé Messdaghi,Eirick Lurass,Casey John Ellis
- BTVT1 - cont...(13:30-14:30 PDT) - [Building BLUESPAWN: An Open-Source, Active Defense & EDR Software \(Intermediate\)](#) - Jake Smith,Jack McDowell
- BTWV1 - cont...(13:30-14:59 PDT) - [Turning Telemetry and Artifacts Into Information \(Intermediate\)](#) - Omenscan
- CHV - [Realistic Trends in Vulnerability based on Hacking into Vehicle](#) - Ryosuke Uematsu,Shogo Nakao,Ryoichi Teramura,Tatsuya Katsuhara
- CHV - [Bluetooth Security in Automotive](#) - Kamel Ghali
- CLV - cont...(13:25-14:10 PDT) - [Can't Touch This: Detecting Lateral Movement in Zero-Touch Environments](#) - Phillip Marlow
- CLV - [Peeling Back the Layers and Peering Through the Clouds with Security Onion](#) - Wes Lambert
- CPV - [How to store sensitive information in 2020?](#) - Mansi Sheth
- CRV - [Pwning Your Resume](#) - Kris Rides
- DC - (14:30-14:59 PDT) - [Finding and Exploiting Bugs in Multiplayer Game Engines](#) - Jack Baker
- DL - [jeopardize](#) - Utku Sen
- ETV - [Models of Privacy Norms](#) - R. Jason Cronk,Ece Gumusel
- HHV - cont...(13:30-14:30 PDT) - [HackerBox 0057 Build Session](#) - Joseph Long (hwbxr)
- HHV - (14:30-14:59 PDT) - [Meetup: PCB Proto and Rework](#) - ShortTie
- HRV - [So You Got an SDR: Common Signals and the Wiki](#) -
- HTS - [40,000 Leagues UUV Death Match](#) - Dr. Nina Kollars
- ICS - cont...(13:45-14:45 PDT) - [The Journey of ICS Project Files - Visibility and Forensics to Exploitation](#) - Nadav Erez
- IOT - (14:15-14:59 PDT) - [Hella Booters: Why IoT Botnets Aren't Going Anywhere](#) - Netspooky
- LBV - cont...(13:00-14:59 PDT) - General Q&A / Drop-in and Chat
- LPV - (14:15-14:45 PDT) - [Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
- MOV - (14:30-15:30 PDT) - [Getting started with the Intervillage badge](#) - Michael Schloh von Bennowitz
- PHVW - cont...(13:00-14:59 PDT) - [Intrusion Analysis and Threat Hunting with Open Source Tools](#) - Jack Mott,Jason Williams,Josh Stroschein
- RGV - [Performance](#) - Daniel Roy
- RTV - cont...(09:30-15:59 PDT) - [Red Team Village CTF - Finals](#) -
- RTV - (14:15-15:15 PDT) - [Grey Hat SSH: SShenanigans](#) - Evan Anderson
- VMV - [Keynote Remarks: Senator Ron Wyden](#) - Ron Wyden
- VMV - (14:30-14:59 PDT) - [Chairman Benjamin Hovland, US Election Assistance Commission](#) - Benjamin Hovland

Friday - 15:00 PDT

[Return to Index](#) - [Locations Legend](#)

[AEV - Talking To Satellites - 101](#) - Eric Escobar

[AIV - Breakout Session](#)

[ASV - API \(in\)Security TOP 10: Guided tour to the Wild Wild World of APIs](#) - David Sopas,Paulo Silva

[BCV - Attacking and Defending Blockchain Nodes](#) - Peter Kacherginsky

[BHV - cont...\(14:30-15:30 PDT\) - Medical Device Vulnerability Disclosure](#) - Chloé Messdaghi,Eirick Lurass,Casey John Ellis

[BHV - \(15:30-15:59 PDT\) - Hacking the Insulin Supply Chain To Save Lives](#) - Anthony DiFranco

[BTVT1 - Indicators of Emulation \(Intermediate\)](#) - Ch33r10

[BTWV2 - Threat Hunting with the Elastic Stack \(Beginner\)](#) - Ben Hughes

[CHV - CAN be super secure: Bit Smashing FTW](#) - Brent Stone

[CHV - Automotive Ethernet for the rest of us](#) - Infenet

[CLV - cont...\(14:10-16:30 PDT\) - Peeling Back the Layers and Peering Through the Clouds with Security Onion](#) - Wes

Lambert

[CPV - Workshop: Let's Talk About Abusability Testing](#) - Avi Zajac,Francesca Spektor, Ji Su Yoo,Nicole Chi

[CRV - In theory, there is no difference between theory and practice](#) - Pablo Breuer

[DC - \(15:30-15:59 PDT\) - Don't Be Silly - It's Only a Lightbulb](#) - Eyal Itkin

[DL - cont...\(14:00-15:50 PDT\) - jeopardize](#) - Utku Sen

[HHV - \(15:30-15:59 PDT\) - Meetup: Legacy Hardware](#) - ShortTie

[ICS - 5 Quick Wins for Improving your ICS Cybersecurity Posture](#) - Austin Scott

[ICS - \(15:45-16:45 PDT\) - PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS](#) - Ben Gardiner

[IOT - \(15:15-16:15 PDT\) - NAND Flash – Recovering File Systems from Extracted Data](#) -

[LBV - Alarm Bypass + Q&A](#)

[LPV - Doors, Cameras, and Mantraps OH MY!](#) - Dylan The Magician

[MOV - cont...\(14:30-15:30 PDT\) - Getting started with the Intervillage badge](#) - Michael Schloh von Bennewitz

[MOV - \(15:30-15:59 PDT\) - Monero Wallet Basics: Sending, Receiving, Proving](#) - rehr

[POV - \(15:30-16:30 PDT\) - Election Security](#) -

[PWDV - Result of Longer Passwords in Real World Application](#) - Minga

[RTV - cont...\(09:30-15:59 PDT\) - Red Team Village CTF - Finals](#) -

[RTV - cont...\(14:15-15:15 PDT\) - Grey Hat SSH: SShenanigans](#) - Evan Anderson

[RTV - \(15:30-16:30 PDT\) - Yippee-Ki-Yay MFA'er - Bypassing Multi-Factor Authentication with Real-Time Replay Session](#)

[Instantiation Attacks](#) - Justin Hutchens (“Hutch”)

[VMV - Secretary Kim Wyman, Washington](#) - Kim Wyman

Friday - 16:00 PDT

[Return to Index - Locations Legend](#)

AEV - [Hack-A-Sat Friday Recap](#) -
AIV - [Workshop 2](#)
ASV - [Threat Modelling the Death Star](#) - Mário Areias
ASV - [JWT Parkour](#) - Louis Nyffenegger
BCV - [Panel Discussion](#)
BHV - (16:15-16:45 PDT) - [Cybersecurity informed consent for medical devices](#) -
BHV - (16:45-17:45 PDT) - [INCLUDES NO DIRT: Threat Modeling for Healthcare](#)
BTVT1 - [Detecting The Not-PowerShell Gang \(Intermediate\)](#) - Mangatas Tondang
BTVW1 - (16:30-17:59 PDT) - [Open-Source Tools for Hunting and Practical Intelligence \(Intermediate\)](#) - Joe Slowik
BTVW2 - cont...(15:00-16:30 PDT) - [Threat Hunting with the Elastic Stack \(Beginner\)](#) - Ben Hughes
CHV - [Misbehavior Detection for V2X communication](#) - Jaime
CHV - [Car \(to Cloud\) Talk: Using MQTT for Car Hacking](#) - Jaime
CLV - cont...(14:10-16:30 PDT) - [Peeling Back the Layers and Peering Through the Clouds with Security Onion](#) - Wes Lambert
CPV - [DNS Privacy](#) - Matt Cheung
CRV - [Building Teams in the New Normal](#) - Mike Murray
DC - (16:30-16:59 PDT) - [Exploiting Key Space Vulnerabilities in the Physical World](#) - Bill Graydon
DL - [redlure](#) - Matthew Creel
ETV - [Security of Election Systems: A contract case study in progress](#) - Rim Boujnah
ICS - cont...(15:45-16:45 PDT) - [PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS](#) - Ben Gardiner
IOT - cont...(15:15-16:15 PDT) - [NAND Flash – Recovering File Systems from Extracted Data](#) -
IOT - (16:45-17:30 PDT) - [Assembling VULNtron: 4 CVEs that Turn a Teleconference Robot into a Spy](#) - Mark Bereza
LBV - cont...(15:00-16:30 PDT) - [Alarm Bypass + Q&A](#)
LBV - (16:30-16:59 PDT) - [General Q&A / Drop-in and Chat](#)
LPV - (16:15-16:45 PDT) - [Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
MOV - [Meme Competition](#)
PHVT - [Take Down the Internet! With Scapy](#) - C8 (John Hammond)
PHVW - [Violent Python 3](#) - Elizabeth Biddlecome, Irvin Lemus, Kaitlyn Handleman, Sam Bowne
POV - cont...(15:30-16:30 PDT) - [Election Security](#) -
PWDV - [From Printers to Silver Tickets or Something](#) - EvilMog
RGV - [Pickpocketing @ Home](#) - James Harrison
RTV - cont...(15:30-16:30 PDT) - [Yippee-Ki-Yay MFA'er - Bypassing Multi-Factor Authentication with Real-Time Replay Session Instantiation Attacks](#) - Justin Hutchens (“Hutch”)
RTV - (16:45-17:45 PDT) - [Enumerating Cloud File Storage Gems](#) - Michael Wylie

Friday - 17:00 PDT

[Return to Index](#) - [Locations Legend](#)

[AEV - Exploiting Spacecraft](#) - Brandon Bailey

[AIV - cont...\(16:00-17:30 PDT\)](#) - Workshop 2

[ASV - cont...\(16:00-17:59 PDT\)](#) - [JWT Parkour](#) - Louis Nyffenegger

[BHV - cont...\(16:45-17:45 PDT\)](#) - [INCLUDES NO DIRT: Threat Modeling for Healthcare](#)

[BTVT1 - Discovering ELK The First Time - Lessons Learned Over 2 Years \(Beginner\)](#) - TheDrPinky

[BTWV1 - cont...\(16:30-17:59 PDT\)](#) - [Open-Source Tools for Hunting and Practical Intelligence \(Intermediate\)](#) - Joe Slowik

[CNE - EFF Tech Trivia Pub Quiz](#) -

[CPV - Fireside Chat: All about Section 230, the EARN IT Act, and What They Mean for Free Speech and Encryption](#) - Cathy Gellis,Riana Pfefferkorn

[CRV - Future Proofing Your Career](#) - Jenai Marinkovic

[DC - \(17:30-17:59 PDT\)](#) - [A Hacker's guide to reducing side-channel attack surfaces using deep-learning](#) - Elie Bursztein

[DL - cont...\(16:00-17:55 PDT\)](#) - [redlure](#) - Matthew Creel

[HHV - \(17:30-17:59 PDT\)](#) - [Meetup: Some HHV Challenges](#) - rehr

[IOT - cont...\(16:45-17:30 PDT\)](#) - [Assembling VULNtron: 4 CVEs that Turn a Teleconference Robot into a Spy](#) - Mark Bereza

[IOT - \(17:45-18:15 PDT\)](#) - [Pandemic In Plaintext](#) - Troy Brown

[PHVW - cont...\(16:00-17:59 PDT\)](#) - [Violent Python 3](#) - Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handleman,Sam Bowne

[RGV - cont...\(16:00-17:59 PDT\)](#) - [Pickpocketing @ Home](#) - James Harrison

[RTV - cont...\(16:45-17:45 PDT\)](#) - [Enumerating Cloud File Storage Gems](#) - Michael Wylie

[WLV - \(17:45-18:45 PDT\)](#) - [Wireless Village Fireside Talk](#) -

Friday - 18:00 PDT

[Return to Index - Locations Legend](#)

[BTVT1 - \(18:30-18:59 PDT\) - Fighting a Virus with a Spreadsheet \(Beginner\)](#) - Allen Baranov

[BTWV2 - Data Analysis for Detection Research Through Jupyter Notebooks 101 \(Beginner\)](#) - Roberto Rodriguez,Jose Rodriguez

[CNE - cont...\(17:00-18:59 PDT\) - EFF Tech Trivia Pub Quiz](#) -

[CNE - War Story Bunker](#) -

[CNE - Hacker Jeopardy](#) -

[DC - \(18:30-18:59 PDT\) - Office Drama on macOS](#) - Patrick Wardle

[ENT - Terrestrial Access Network](#) -

[HHV - Meetup: 3H: Hardware Happy Hour](#) - Chris Gammell

[IOT - cont...\(17:45-18:15 PDT\) - Pandemic In Plaintext](#) - Troy Brown

[IOT - \(18:30-19:15 PDT\) - The Joy of Coordinating Vulnerability Disclosure](#) - Daniel Gruss,CRob,Lisa Bradley,Katie Noble,Omar Santos, Anders Fogh

[PWDV - Getting Advanced with Hashcat](#) - Password Village Staff

[RTV - Total E\(A\)gression](#) - Alvaro Folgado Rueda

[WLV - cont...\(17:45-18:45 PDT\) - Wireless Village Fireside Talk](#) -

Friday - 19:00 PDT

[Return to Index](#) - [Locations Legend](#)

[BTVT1](#) - (19:30-20:30 PDT) - [Purple On My Mind: Cost Effective Automated Adversary Simulation \(Intermediate\)](#) - Mauricio Velazco

[BTWV2](#) - cont...(18:00-19:30 PDT) - [Data Analysis for Detection Research Through Jupyter Notebooks 101 \(Beginner\)](#) - Roberto Rodriguez, Jose Rodriguez

[CNE](#) - cont...(18:00-19:59 PDT) - [War Story Bunker](#) -

[CNE](#) - cont...(18:00-19:59 PDT) - [Hacker Jeopardy](#) -

[ENT](#) - [Acid T](#) -

[IOT](#) - cont...(18:30-19:15 PDT) - [The Joy of Coordinating Vulnerability Disclosure](#) - Daniel Gruss, CRob, Lisa Bradley, Katie Noble, Omar Santos, Anders Fogh

[RTV](#) - (19:15-20:15 PDT) - [Password cracking beyond 15 characters and under \\$500](#) - Travis Palmer

Friday - 20:00 PDT

[Return to Index - Locations Legend](#)

[BTVT1 - cont...\(19:30-20:30 PDT\) - Purple On My Mind: Cost Effective Automated Adversary Simulation \(Intermediate\) -](#)

Mauricio Velazco

[ENT - Ictre Normal -](#)

[FSL - D0 N0 H4RM: A Healthcare Security Conversation - Ash Luft,Christian "quaddi" Dameff,Jeff "r3plicanTully,Suzanne Schwartz,Vidya Murthy](#)

[RTV - cont...\(19:15-20:15 PDT\) - Password cracking beyond 15 characters and under \\$500 - Travis Palmer](#)

[RTV - \(20:30-21:30 PDT\) - 50 Shades of Sudo Abuse - Tyler Boykin](#)

[VMV - Live Q&A with Special Guests Regarding "Kill Chain" -](#)

[ENT - Zebbler Encanti Experience](#) -

[FSL - Shrek, Jugs, and Toxic Trolls: a BADASS discussion about Online Sexuality and Hacktivism](#) - Katelyn

Bowden,Rachel Lamp,Allie Barnes,Kate Venable,Marleigh Farlow,Tim Doomsday

[PWDV - Getting Started with Hashcat \(Rebroadcast\)](#) - Password Village Staff

[PWDV - \(21:30-21:59 PDT\) - Making Targeted Wordlists \(Rebroadcast\)](#) - Password Village Staff

[RTV - cont...\(20:30-21:30 PDT\) - 50 Shades of Sudo Abuse](#) - Tyler Boykin

[RTV - \(21:45-22:45 PDT\) - ATTPwn: Adversarial Emulation and Offensive Techniques Collaborative Project](#) - Fran

Ramirez,Pablo Gonzalez

[Return to Index - Locations Legend](#)

ENT - Ninjula -

PWDV - [Result of Longer Passwords in Real World Application \(Rebroadcast\)](#) - Minga

PWDV - (22:30-22:40 PDT) - [From Printers to Silver Tickets or Something \(Rebroadcast\)](#) - EvilMog

PWDV - (22:40-23:30 PDT) - [Getting Advanced with Hashcat \(Rebroadcast\)](#) - Password Village Staff

RTV - cont...(21:45-22:45 PDT) - [ATTPwn: Adversarial Emulation and Offensive Techniques Collaborative Project](#) - Fran Ramirez,Pablo Gonzalez

[Return to Index - Locations Legend](#)

[ENT - Shadowvex -](#)

[PWDV - cont...\(22:40-23:30 PDT\) - Getting Advanced with Hashcat \(Rebroadcast\) - Password Village Staff](#)

[RTV - ERPwnage - a red team approach to targeting SAP - Austin Marck](#)

Friday - 8:00 PDT

[Return to Index - Locations Legend](#)

[CLV - cont...\(06:00-12:30 PDT\) - Cloud Village CTF -](#)

Friday - 9:00 PDT

[Return to Index - Locations Legend](#)

CLV - cont...(06:00-12:30 PDT) - [Cloud Village CTF](#) -

Saturday

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

Saturday - 00:00 PDT

[Return to Index](#) - [Locations Legend](#)

[PWDV - PathWell: Dynamic Password Strength Enforcement \(Rebroadcast\)](#) - Hank Leininger

[RTV - Back to the future: Computer science and systems biology](#) - Dr Lorenz Adlung, Noa Novogroder

[Return to Index - Locations Legend](#)

RTV - (02:15-03:15 PDT) - [Modern Red Team Tradecraft - Informing Defenders by Evolving Your Attackers](#) - Sajal Thomas

[Return to Index - Locations Legend](#)

[RTV - cont...\(02:15-03:15 PDT\) - Modern Red Team Tradecraft - Informing Defenders by Evolving Your Attackers](#) - Sajal Thomas

[RTV - \(03:30-04:30 PDT\) - Executing Red Team Scenarios with Built-in Scenario Place](#) - Erdener Uyan,Gökberk Gülgin

[Return to Index - Locations Legend](#)

[RTV - cont...\(03:30-04:30 PDT\) - Executing Red Team Scenarios with Built-in Scenario Place](#) - Erdener Uyan,Gökberk Gülğün

[RTV - \(04:45-05:45 PDT\) - OU having a laugh?](#) - Petros Koutroumpis

[Return to Index - Locations Legend](#)

RTV - cont...(04:45-05:45 PDT) - [OU having a laugh?](#) - Petros Koutroumpis

[Return to Index - Locations Legend](#)

RTV - All of the threats: Intelligence, modelling and hunting through an ATT&CKers lens - Tim Wadhwa-Brown

[Return to Index - Locations Legend](#)

RTV - (07:15-08:15 PDT) - [Catch Me if You Can](#) - Eduardo Arriols

[Return to Index - Locations Legend](#)

- [AEV - \(08:30-08:59 PDT\) - Attacking Flight Management Systems: This Is Your Captain Speaking, We Have A Small Problem!](#) - Javad Dadgar, Mohammad-Reza Zamiri, Reza Dorosti
- [HHV - \(08:30-08:59 PDT\) - Learn to Solder the BadgeBuddy Kit](#) - Joseph Long (hwbxr)
- [RTV - cont...\(07:15-08:15 PDT\) - Catch Me if You Can](#) - Eduardo Arriols
- [RTV - \(08:30-09:30 PDT\) - Mechanizing the Methodology: Automating Discovery, Testing, and Alerting using Recon/Testing Tools and Amazon SES](#) - Daniel Miessler

[Return to Index - Locations Legend](#)

[AEV - Hack-A-Sat Kickoff Segment -](#)

[AEV - \(09:30-09:59 PDT\) - Aerospace Village Badge - Rick Hansen](#)

[AIV - \(09:30-09:59 PDT\) - "SECRETS ARE LIES, SHARING IS CARING, PRIVACY IS THEFT."- A Dive into Privacy Preserving Machine Learning - Nahid Farhady](#)

[ASV - Be Like Water: What Bruce Lee Can Teach Us About AppSec - Fredrick "Flee" Lee](#)

[BTVT1 - Reversing with Dynamic Data Resolver \(DDR\) – Best practice \(Advanced\) - Holger Unterbrink](#)

[BTWV1 - Leveraging the critical YARA skills for Blue Teamers \(Beginner\) - David Bernal Michelena](#)

[DC - \(09:30-09:59 PDT\) - A Decade After Stuxnet's Printer Vulnerability: Printing is still the Stairway to Heaven - Peleg Hadar, Tomer Bar](#)

[HHV - \(09:30-09:59 PDT\) - Hardware hacking 101: There is plenty of room at the bottom - Federico Lucifredi](#)

[ICS - ICS SecOps: Active Defense Concept with Effective Incident Response in Industrial Control Systems](#)

[ICS - \(09:45-10:45 PDT\) - Confessions of an Offensive ICS Cyber Security Researcher - Marina Krotofil](#)

[IOT - Hacking smart-devices for fun and profit: From exploiting my smart-home into controlling thousands of smart-devices around the world - Barak Sternberg](#)

[PHVW - Writing Wireshark Plugins for Security Analysis - Jeswin Mathai, Nishant Sharma](#)

[RTV - cont...\(08:30-09:30 PDT\) - Mechanizing the Methodology: Automating Discovery, Testing, and Alerting using Recon/Testing Tools and Amazon SES - Daniel Miessler](#)

[RTV - \(09:45-10:45 PDT\) - Y'all Tryna Bypass Python 3.8 Audit Hooks or Nah? - Leron Gray](#)

[AEV - Hackers And ISACS](#) - Erin Miller,Jeff Troy,Ken Munro,Matthew Gaffney,Pete Cooper
[AIV - Misinformation & Covid](#) - Imeyerov
[ASV - Web Shell Hunting - Part 1](#) - Joe Schottman
[ASV - 10,000 Dependencies Under The Sea: Exploring and Securing Open source dependencies](#) - Gregg Horton,Ryan Slama
[BCV - Welcome Note](#)
[BCV - Twitter's Tax Day Disaster: The Beginning \(and End\) of Mainstream Crypto Scams](#) - Victor Fang
[BHV - DAY2 KEYNOTE: Understanding DIYBio and Community Labs - A Social Science Approach](#) - Yong-Bee
[BTVT1 - \(10:30-10:59 PDT\) - O365Squatting \(Intermediate\)](#) - Juan Francisco,Jose Miguel Gómez-Casero Marichal
[BTWV1 - cont...\(09:00-10:30 PDT\) - Leveraging the critical YARA skills for Blue Teamers \(Beginner\)](#) - David Bernal Michelena
[BTWV2 - \(10:30-11:59 PDT\) - Wireshark for Incident Response & Threat Hunting \(Beginner\)](#) - Michael Wylie
[CHV - Hacking TESLA Model 3 - NFC Relay Revisited](#) - Huajiang "Kevin2600" Chen,Yuchao (Alex) Zhang
[CHV - Automotive In-Vehicle Networks](#) - Kamel Ghali
[CPV - Quantum Computers & Cryptography](#) - I. Shaheem
[CRV - Cons and Careers](#) - Steven Bernstein
[DC - \(10:30-10:59 PDT\) - Whispers Among the Stars: Perpetrating \(and Preventing\) Satellite Eavesdropping Attacks](#) - James Pavur
[DCG - OWASP API Top 10](#) -
[DL - jeopardize](#) - Utku Sen
[DL - Starkiller](#) - Vincent "Vinnybod" Rose
[ETV - Killer Robots Reconsidered](#) - Diane Vavrichek,Larry Lewis
[HRV - Single Board Computers in Amateur Radio](#) -
[HTS - Speed 2: The Poseidon Adventure – When Cruise Ships Go Wrong](#) - Andrew Tierney
[ICS - cont...\(09:45-10:45 PDT\) - Confessions of an Offensive ICS Cyber Security Researcher](#) - Marina Krotofil
[IOT - Your connected world isn't yours anymore! - Remote IoT attacks and data exfiltration.](#) - Dewank Pant,Shruti Lohani
[LPV - Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
[LPV - \(10:45-11:45 PDT\) - High Security Wafer Locks - An Oxymoron?](#) - zeefeene
[MOV - Keynote: Monero: Sound Money Safe Mode](#) - Dr. Daniel Kim
[PAYV - Identity Crisis: the mad rise of online account opening fraud](#) - Uri Rivner
[PHVT - The Vulnerability That Gmail Overlooked and Enabling Threat Hunting](#) - Özkan Mustafa Akkus
[PHVW - cont...\(09:00-10:59 PDT\) - Writing Wireshark Plugins for Security Analysis](#) - Jeswin Mathai,Nishant Sharma
[PWDV - Cracking at Extreme Scale: The Evolution of Hashstack](#) - Jeremi M Gosney (epixoip)
[RCV - Twitter Word Phrequency](#) - Master Chen
[RTV - cont...\(09:45-10:45 PDT\) - Y'all Tryna Bypass Python 3.8 Audit Hooks or Nah?](#) - Leron Gray
[VMV - War By Other Means: How Influence Operations Undermine Democracy](#) - Ben Dubow
[VMV - \(10:30-10:59 PDT\) - John Odum, Montpelier, VT](#) - John Odum

[Return to Index - Locations Legend](#)

AEV - [A View From The Cockpit: Exploring Pilot Reactions To Attacks On Avionic Systems](#) - Matt Smith
AEV - (11:30-11:59 PDT) - [Checklist For Aviation Vulnerability Disclosure: Don't Go It Alone](#) - Jay Angus
AIV - [Workshop 3](#)
ASV - [Hackium: a browser for web hackers](#) - Jarrod Overson
BCV - [Decentralized Finance \(DeFi\) - ready for prime time ?](#) - Ryan Rubin
BHV - [How COVID19 Changed Our Understanding of Cyber Disaster Medicine](#) - Christian “quaddi” Dameff, Jeff “r3plicant” Tully
BTVT1 - (11:30-11:59 PDT) - [Low Value Indicators For High Value Decisions \(Intermediate\)](#) - Allan Stojanovic, Spencer Cureton
BTVW2 - cont...(10:30-11:59 PDT) - [Wireshark for Incident Response & Threat Hunting \(Beginner\)](#) - Michael Wylie
CHV - [OBD and what we CAN do with it](#) - Infernet
CLV - [Least privilege using infrastructure as code](#) - Nimrod Kor
CLV - (11:45-12:30 PDT) - [How Blue Penetrates You](#) - Dani Goland, Mohsan Farid
CPV - [Online Ads as a Recon and Surveillance Tool](#) - Neil M
CPV - (11:30-11:59 PDT) - [Who needs spyware when you have COVID-19 apps? A look at global trends and what to do about it.](#) - C. Nadal, J. DeBlois, M. DeBlois, Z. Anderson
CRV - [The Individual Contributor to Tech Executive, or There and Back Again](#) - Amelie Koran
DC - (11:30-11:59 PDT) - [Don't Ruck Us Again - The Exploit Returns](#) - Gal Zror
DCG - [Government Espionage on a School Lunch Budget](#) -
DL - cont...(10:00-11:50 PDT) - [jeopardize](#) - Utku Sen
DL - cont...(10:00-11:50 PDT) - [Starkiller](#) - Vincent “Vinnybod” Rose
HHV - [onkeypress=hack\(\);](#) - Farith Pérez Sáez, Luis Ángel Ramírez Mendoza (@larm182luis), Mauro Cáseres
HRV - (11:30-12:30 PDT) - [Discussion: What makes a good ham radio operator?](#) -
HTS - [Hack the SeaPod](#) - Grant Romundt
ICS - [Playing with Electricity: Hacking into Distribution Companies](#) - Can Demirel, Serkan Temel
IOT - [Introduction to U-Boot Interaction and Hacking](#) - Garrett Enoch
LBV - [Bypass 101 + Q&A](#)
LPV - cont...(10:45-11:45 PDT) - [High Security Wafer Locks - An Oxymoron?](#) - zeefeene
MOV - cont...(10:00-11:30 PDT) - [Keynote: Monero: Sound Money Safe Mode](#) - Dr. Daniel Kim
PAYV - [Online Banking Security](#) - Arkadiy Litvinenko
POV - [AMA w/@hackingdave & @kennwhite](#) - hackingdave, kennwhite
RCV - [Burnout is real](#) - Chloé Messdaghi
RTV - [Initial Compromise through Web Side](#) - Walter Cuestas
VMV - [Heightened Election Security Risks Admist the Pandemic](#) - Jack Cable, Alex Zaheer
VMV - (11:30-11:59 PDT) - [Hack-a-Fax](#) - Forrest Senti, Mattie Gullixson, Caleb Gardner

[AEV - Low-Cost VHF Receiver: Eavesdropping Pilot/Controller Communication](#) - Allan Tart,Fabian Landis
[AIV - cont...\(11:00-12:30 PDT\) - Workshop 3](#)
[ASV - The DevOps & Agile Security Toolkit](#) - David Waldrop
[ASV - Web Shell Hunting - Part 2](#) - Joe Schottman
[BCV - Securing the COSMOS: How to operate and secure a validator](#) - Ron Stoner
[BHV - Medical Technology: How do we unfuck things](#) - Veronica
[BHV - \(12:30-13:30 PDT\) - Advancing Medical Device Security – How collaboration between providers, manufacturers, and pen testers is advancing what’s possible with security.](#) - Mitchell Parker
[BTVT1 - \(12:30-13:30 PDT\) - Incident Response Panel](#) - Russell Mosley,Vyrus,Litmoose,Xavier Ashe
[BTVW1 - Tracer FIRE 9 \(Intermediate\)](#) - Andrew Chu
[CHV - Houston, we CAV a problem](#) - Vic Harkness
[CHV - Fundamentals of Diagnostic Requests over CAN Bus](#) - Robert Leale (CarFuCar)
[CLV - cont...\(11:45-12:30 PDT\) - How Blue Penetrates You](#) - Dani Goland,Mohsan Farid
[CLV - \(12:30-13:15 PDT\) - 21 Jump Server: Going Bastionless in the Cloud](#) - Colin Estep
[CPV - Differential Privacy..more important than ever in the world of Covid-19](#) - Aditi Joshi
[CRV - Entrepreneurial Adventures: What It Takes to Start A Company](#) - Bryson Bort
[DC - \(12:30-12:59 PDT\) - Applied Ca\\$h Eviction through ATM Exploitation](#) - Brenda So,Trey Keown
[DCG - Basic OSINT: Mining Personal Data](#) -
[DL - Phirautee](#) - Viral Maniar
[ETV - Vote @ Home Workshop](#) - Andrea Matwyshyn
[HHV - Learn to Solder the BadgeBuddy Kit](#) - Joseph Long (hwbxr)
[HRV - cont...\(11:30-12:30 PDT\) - Discussion: What makes a good ham radio operator?](#) -
[ICS - \(12:15-13:15 PDT\) - Vivisecting PowerPC](#) - ac0rn,atlas 0f d00m
[IOT - \(12:30-13:15 PDT\) - Kicking Devices and Taking CVEs : The Zoomer’s Guide to Hacking Shit](#) - Sanjana Sarda
[LBV - cont...\(11:00-12:30 PDT\) - Bypass 101 + Q&A](#)
[LBV - \(12:30-13:59 PDT\) - Alarm Bypass + Q&A](#)
[LPV - Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
[MOV - Open Office Q&A w/ Monero Research Lab's Sarang](#) - Sarang
[PAYV - Trends in the online card payment security](#) - Dr Mohammed Aamir Ali
[PWDV - What the Shuck? Layered Hash Shucking](#) - Sam Croley (Chick3nman)
[RCV - Hunting for Blue Mockingbird Coinminers](#) - Ladislav B
[RTV - \(12:15-12:30 PDT\) - Inside the Mind of a Threat Actor: Beyond Pentesting](#) - Phillip Wylie
[RTV - \(12:45-13:45 PDT\) - The Student Roadmap to Becoming A Penetration Tester](#) - Jonathan Helmus
[VMV - Analysis of the Attack Data Collected During Mobile Voting Pilots](#) - Nimit Sawhney,Nailah Mims
[VMV - \(12:30-12:59 PDT\) - Remote Online Balloting Delivery and Marking Options and Security Considerations for Absentee Voting During the COVID-19 Pandemic](#) - Susan Greenhalgh,Steve Newell

[AEV - Product Cybersecurity: Secure Airplane Development Lifecycle](#) - Michael Vanguardia
[AEV - \(13:30-13:59 PDT\) - Introduction To ACARS](#) - Alex Lomas
[AIV - Journal Club Live! Fawkes FR](#) - AI Village Journal Club
[ASV - cont...\(12:00-13:59 PDT\) - Web Shell Hunting - Part 2](#) - Joe Schottman
[ASV - localghost: Escaping the Browser Sandbox Without 0-Days](#) - Parsia Hakimian
[BCV - Blockchain for Cyber Defense: Will it be as good as you think?](#) - Seungjoo,Suhyeon Lee
[BCV - \(13:30-13:59 PDT\) - Identifying and fixing out-of-gas errors in smart contracts with smart fuzzing](#) - Sebastian Banescu
[BHV - cont...\(12:30-13:30 PDT\) - Advancing Medical Device Security – How collaboration between providers, manufacturers, and pen testers is advancing what’s possible with security.](#) - Mitchell Parker
[BTVT1 - cont...\(12:30-13:30 PDT\) - Incident Response Panel](#) - Russell Mosley,Vyrus,Litmoose,Xavier Ashe
[BTWV1 - cont...\(12:00-13:30 PDT\) - Tracer FIRE 9 \(Intermediate\)](#) - Andrew Chu
[BTWV2 - \(13:30-15:30 PDT\) - An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology \(Beginner\)](#) - Ben Bornholm
[CHV - CMAP: Open Source Vehicle Services Mapping Tool for noobs](#) - Robert Leale (CarFuCar)
[CHV - Cluster fuzz!](#) - Mintynet
[CLV - cont...\(12:30-13:15 PDT\) - 21 Jump Server: Going Bastionless in the Cloud](#) - Colin Estep
[CLV - \(13:15-13:59 PDT\) - Cloud Frontier](#) - Setu Parimi
[CNE - Film Festival: Project Immerse: A Deepfake Paranoid Thriller](#) -
[CPV - Rights You Can’t Exercise Can’t Protect You: Privacy by Design, Dark Patterns, and Cultural Context](#) - Ben Brook,Maritza Johnson,Megan DeBlois,Zach Singleton
[CRV - National Service Panel: Career Opportunities Supporting the Country](#) - John Felker,Diane Janosek,Chris Pimlott,Roman Vitkovitsky,Liz Popiak,Joe Billingsley
[DC - \(13:30-13:59 PDT\) - How we recovered \\$XXX,000 in Bitcoin from an encrypted zip file](#) - Michael Stay
[DCG - Intro to DC858](#) -
[DCG - \(13:15-13:59 PDT\) - Saving Yourself from Microsoft: It's by design](#) -
[DL - cont...\(12:00-13:50 PDT\) - Phirautee](#) - Viral Maniar
[ETV - cont...\(12:00-14:10 PDT\) - Vote @ Home Workshop](#) - Andrea Matwyshyn
[HHV - Meetup: Some HHV Challenges](#) - rehr
[HRV - \(13:30-13:59 PDT\) - Practice 'Net' via Discord](#) -
[ICS - cont...\(12:15-13:15 PDT\) - Vivisecting PowerPC](#) - ac0rn,atlas Of d00m
[ICS - \(13:30-13:59 PDT\) - MITRE ICS ATT&CK](#) - Marie,Otis
[IOT - cont...\(12:30-13:15 PDT\) - Kicking Devices and Taking CVEs : The Zoomer’s Guide to Hacking Shit](#) - Sanjana Sarda
[IOT - \(13:45-14:15 PDT\) - In search of the perfect UPnP tool](#) - Trevor Stevado t1v0
[LBV - cont...\(12:30-13:59 PDT\) - Alarm Bypass + Q&A](#)
[LPV - Law School for Lockpickers](#) - Preston Thomas
[MOV - \(13:30-14:30 PDT\) - Badge Clinic](#) - Michael Schloh von Bennewitz
[PHVT - The Worst Mobile Apps](#) - Sam Bowne
[PHVW - Wireshark for Incident Response & Threat Hunting](#) - Michael Wylie
[PWDV - PathWell: Dynamic Password Strength Enforcement](#) - Hank Leininger
[RCV - Ambly, the Smart Darknet Spider](#) - Levi
[RTV - cont...\(12:45-13:45 PDT\) - The Student Roadmap to Becoming A Penetration Tester](#) - Jonathan Helmus
[VMV - Don’t Go Postal Over Mail In Voting](#) - Bianca Lewis
[VMV - \(13:30-13:59 PDT\) - The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections](#) - Michael A. Specter

[Return to Index - Locations Legend](#)

- [AEV - Ticketing To Takeoff: An Airport Hacking Choose Your Own Adventure](#) - Liz Wharton
- [AIV - Does AI Live up to the Hype?](#)
- [BCV - Monetary Maximalism and Millennial Finance - Building Decentralized Tooling to Empower Everyone](#) - Kris Jones, Matt Luongo
- [BHV - MedICS](#) - Bryson Bort
- [BHV - \(14:45-15:15 PDT\) - Towards an Institutional Review Board for Biohackers](#) - Dr. Sarah Blossom Ware
- [BTVT1 - Blue Team Village & Red Team Village Panel](#) - Joseph Mlodzianowski (cedoXx), Adam Mashinchi, Plug, Dani, Jorge Orchilles, David J. Bianco
- [BTVW2 - cont...\(13:30-15:30 PDT\) - An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology \(Beginner\)](#) - Ben Bornholm
- [CHV - All Aboard the CAN Bus... or Motorcycle](#) - Derrick (CanBusDutch)
- [CHV - Bluetooth Security in Automotive](#) - Kamel Ghali
- [CLV - Attacking the Helmsman](#) - Mohit Gupta
- [CLV - \(14:45-15:30 PDT\) - SaaSocalypse - The Complexity and Power of AWS Cross Account Access](#) - Alexandre Sieira
- [CNE - cont...\(13:00-14:30 PDT\) - Film Festival: Project Immerse: A Deepfake Paranoid Thriller](#) -
- [CPV - Hacking like Paris Hilton 14 years later - and still winning!](#) - Per Thorsheim
- [CRV - Veteran Transition Tips](#) - Bob Wheeler
- [DC - \(14:30-14:59 PDT\) - Abusing P2P to Hack 3 Million Cameras: Ain't Nobody Got Time for NAT](#) - Paul Marrapese
- [DCG - Understanding the Threat: Malicious Software, Malicious Actors, and the Promise of Connected Medical Technology](#) -
- [DL - PyRDP: Remote Desktop Protocol Monster-in-the-Middle \(MITM\) and Library](#) - Olivier Bilodeau, Alexandre Beaulieu
- [ETV - cont...\(12:00-14:10 PDT\) - Vote @ Home Workshop](#) - Andrea Matwyshyn
- [ETV - Federal Trade Commision](#) - Comm. Rohit Chopra
- [HHV - Meetup: Sourcing Parts](#) - bombnav
- [HRV - Ham Radio USA License Exams \(Saturday\)](#) -
- [ICS - \(14:15-15:15 PDT\) - Building a Physical Testbed for Blackstart Restoration under Cyber Fire](#) - Tim Yardley
- [IOT - cont...\(13:45-14:15 PDT\) - In search of the perfect UPnP tool](#) - Trevor Stevado t1v0
- [IOT - \(14:30-15:20 PDT\) - The future of IoT Security "Baselines, Standards, and Regulatory Domain](#) - Amit Elazari, Anahit Tarkhanyan
- [LBV - Reconnaissance + Q&A](#)
- [LPV - \(14:15-14:45 PDT\) - Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
- [MOV - cont...\(13:30-14:30 PDT\) - Badge Clinic](#) - Michael Schloh von Bennewitz
- [PHVW - cont...\(13:00-14:59 PDT\) - Wireshark for Incident Response & Threat Hunting](#) - Michael Wylie
- [POV - AMA w/Policymakers](#) -
- [PWDV - Practical PCFG Password Cracking](#) - Matt Weir
- [RCV - COVID 1984_ Propaganda and Surveillance during a Pandemic](#) - Mauro Cáseres
- [RGV - Performance](#) - Daniel Roy
- [RTV - \(14:15-14:59 PDT\) - The Art of Balancing: A Burnout Talk](#) - Chloé Messdaghi
- [VMV - Vote-from-home? Review of Election Security on Remote Voting in Response to COVID-19](#) - Sang-Oun Lee
- [VMV - \(14:30-14:59 PDT\) - Electronic Ballot Return Standards & Guidelines](#) - Forrest Senti, Mattie Gullixson

- [AEV - ILS and TCAS Spoofing Demonstration](#) - Alex Lomas
- [AEV - \(15:30-15:59 PDT\) - A Deeper Dive Into ILS And ADS-B Spoofing](#) - Harshad Sathaye
- [AIV - AI vs. Airplanes and IT-Security: What Security Regulations Teach Us About AI Governance](#) - Laurin Weissinger
- [ASV - Can't Touch This: Detecting Lateral Movement in Zero-Touch Environments](#) - Phillip Marlow
- [BCV - 7 Phases of Smart Contract Hacking](#) - Martin Abbatemarco
- [BHV - cont...\(14:45-15:15 PDT\) - Towards an Institutional Review Board for Biohackers](#) - Dr. Sarah Blossom Ware
- [BHV - \(15:15-15:59 PDT\) - DIY Diabetics and a Million Boluses](#) - Dr. Mike Rushanan, Julian Suleder
- [BTVT1 - \(15:30-16:30 PDT\) - Practical Advice on Threat Hunting Panel](#) - Plug, Roberto Rodriguez, Tony M Lambert, Valentina Palacín, Samir, Ruth Barbacil, Anna McAbee, Paul Melson
- [BTVW1 - \(15:30-16:15 PDT\) - Defending Your UNIX Hosts \(Intermediate\)](#) - Daniel Ward, Samuel Gasparro
- [BTVW2 - cont...\(13:30-15:30 PDT\) - An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology \(Beginner\)](#) - Ben Bornholm
- [CHV - From Blackbox to Automotive Ransomware](#) - Nils Weiss, Enrico Pozzobon
- [CHV - Automotive Ethernet for the rest of us](#) - Infenet
- [CLV - cont...\(14:45-15:30 PDT\) - SaaSocalypse - The Complexity and Power of AWS Cross Account Access](#) - Alexandre Seira
- [CLV - \(15:30-17:30 PDT\) - Discovering Cloud File Storage Artifacts](#) - Michael Wylie
- [CPV - Online Voting: Theory and Practice](#) - Emily Stamm, Porter Adams
- [CRV - Drinks with Recruiters](#) - Kris Rides, Rachel Bozeman, Matt Duren, Pete Radloff
- [DC - \(15:30-15:59 PDT\) - Bypassing Biometric Systems with 3D Printing and Enhanced Grease Attacks](#) - Yamila Levalle
- [DCG - Intro to DC603](#) -
- [DCG - \(15:15-15:59 PDT\) - DNS New World Order, version 1.4: QuadX! DoH! DoT! Da Fuq?](#) -
- [DL - cont...\(14:00-15:50 PDT\) - PyRDP: Remote Desktop Protocol Monster-in-the-Middle \(MITM\) and Library](#) - Olivier Bilodeau, Alexandre Beaulieu
- [ETV - cont...\(14:10-15:20 PDT\) - Federal Trade Commission](#) - Comm. Rohit Chopra
- [ETV - \(15:20-16:30 PDT\) - Food and Drug Administration](#) - Jessica Wilkerson
- [HHV - Meetup: OSS ASIC](#) - Josh Marks
- [HRV - cont...\(14:00-16:59 PDT\) - Ham Radio USA License Exams \(Saturday\)](#) -
- [HRV - OSTWERK Initiative](#) -
- [ICS - cont...\(14:15-15:15 PDT\) - Building a Physical Testbed for Blackstart Restoration under Cyber Fire](#) - Tim Yardley
- [ICS - \(15:30-16:30 PDT\) - Operationalizing Cyber Norms: Critical Infrastructure Protection](#) - Chris Kubecka
- [IOT - cont...\(14:30-15:20 PDT\) - The future of IoT Security “Baselines, Standards, and Regulatory Domain](#) - Amit Elazari, Anahit Tarkhanyan
- [IOT - \(15:30-16:30 PDT\) - Learning to Use Logic Analyzers](#) - Jonathan Stines
- [LBV - cont...\(14:00-15:30 PDT\) - Reconnaissance + Q&A](#)
- [LBV - \(15:30-16:59 PDT\) - Bypass 101 + Q&A](#)
- [LPV - Bobby Pins, More Effective Than Lockpicks?](#) - John the Greek
- [MOV - Decentralization in a Centralized world](#) - rehr
- [RTV - \(15:15-16:15 PDT\) - APTs <3 PowerShell and Why You Should Too](#) - Anthony Rose, Jake “Hubbl3 Krasnov
- [VMV - Understanding Cyber-Attacks and Their Implications to Democratic Regimes](#) - Javier F. Patiño García
- [VMV - \(15:30-15:59 PDT\) - A Lawyer's Reflections on Elections](#) - Cordero Alexander Delgado

- AEV - [Hack-A-Sat End Of Day Recap](#) -
- AIV - [Workshop 4](#)
- BCV - [Panel Discussion](#)
- BHV - [Chinese Military Laboratory Mission + COVID-19](#) - The Red Dragon
- BHV - (16:30-17:30 PDT) - [What's up with proposed privacy legislation and how to influence the debate](#) - Lucia Savage
- BTVT1 - cont...(15:30-16:30 PDT) - [Practical Advice on Threat Hunting Panel](#) - Plug,Roberto Rodriguez,Tony M Lambert,Valentina Palacín,Samir,Ruth Barbacil,Anna McAbee,Paul Melson
- BTVW1 - cont...(15:30-16:15 PDT) - [Defending Your UNIX Hosts \(Intermediate\)](#) - Daniel Ward,Samuel Gasparro
- BTVW2 - (16:30-17:59 PDT) - [A N00b's Intro to Building Your Own Lab \(Beginner\)](#) - Omar Santos
- CHV - [ChupaCarBrah: Open Source Hardware and Software for Interacting with your Vehicle CAN Bus](#) - Marcelo Sacchetin
- CHV - [Car \(to Cloud\) Talk: Using MQTT for Car Hacking](#) - Jaime
- CLV - cont...(15:30-17:30 PDT) - [Discovering Cloud File Storage Artifacts](#) - Michael Wylie
- CPV - [Next level stalker ware](#) - Cecilie Wian
- DC - (16:30-16:59 PDT) - [Reverse Engineering the Tesla Battery Management System for Moar Powerrr!](#) - Patrick Kiley
- DL - [CIRCO v2: Cisco Implant Raspberry Controlled Operations](#) - Emilio Couto
- DL - [Cotopaxi: IoT Protocols Security Testing Toolkit](#) - Jakub Botwicz
- ETV - cont...(15:20-16:30 PDT) - [Food and Drug Administration](#) - Jessica Wilkerson
- ETV - (16:30-17:40 PDT) - [TechCongress](#) - Leisel Bogan
- HHV - [Meetup: Certification Processes \(UL, FCC, etc.\)](#) - ShortTie
- HRV - cont...(14:00-16:59 PDT) - [Ham Radio USA License Exams \(Saturday\)](#) -
- ICS - cont...(15:30-16:30 PDT) - [Operationalizing Cyber Norms: Critical Infrastructure Protection](#) - Chris Kubecka
- ICS - (16:45-17:15 PDT) - [Industrial Cybersecurity in Mexico](#) - Octavio Fernandez,Victor Gomez
- IOT - cont...(15:30-16:30 PDT) - [Learning to Use Logic Analyzers](#) - Jonathan Stines
- LBV - cont...(15:30-16:59 PDT) - [Bypass 101 + Q&A](#)
- LPV - (16:15-16:45 PDT) - [Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
- MOV - [Tricky Bundles: Smarter Dependency Management for I2P-Bundling Applications](#) - idk
- MOV - (16:30-16:59 PDT) - [Kahoot! Quiz](#)
- PHVW - [Advanced APT Hunting with Splunk](#) - Matt Toth,Robert Wagner
- POV - [Mis/Dis Information & Democracy](#) -
- RGV - [Outs, Forces, and Equivoque: A treatise on how Magicians speak](#) - Brandon Martinez
- RTV - cont...(15:15-16:15 PDT) - [APTs <3 PowerShell and Why You Should Too](#) - Anthony Rose,Jake "Hubbl3 Krasnov
- RTV - (16:30-17:30 PDT) - [Indicators of Emulation: Extra Spicy Adversary Emulation](#) - Ch33r10,haydnjohnson
- VMV - [Protecting Elections with Data Science -- A Tool for 2020 and Beyond](#) - Stephanie Singer

[Return to Index - Locations Legend](#)

[AEV - General Aviation \(GA\) Electronic Flight Bags \(EFB\)](#) - David Robinson

[AIV - cont...\(16:00-17:30 PDT\)](#) - Workshop 4

[BHV - cont...\(16:30-17:30 PDT\)](#) - [What's up with proposed privacy legislation and how to influence the debate](#) - Lucia Savage

[BTVT1 - Introducing the Meet a Mentor Program](#) - Scoubi,Plug,Litmoose,Xavier

Ashe,Rand0h,Muteki,PacketSqueezins,ttheveii0x,Allie Hansen,nohackme

[BTWV2 - cont...\(16:30-17:59 PDT\)](#) - [A N00b's Intro to Building Your Own Lab \(Beginner\)](#) - Omar Santos

[CLV - cont...\(15:30-17:30 PDT\)](#) - [Discovering Cloud File Storage Artifacts](#) - Michael Wylie

[CPV - Workshop: Let's Talk About Abusability Testing](#) - Avi Zajac,Franchesca Spektor, Ji Su Yoo,Nicole Chi

[DC - \(17:30-17:59 PDT\)](#) - [Getting Shells on z/OS with Surrogat Chains](#) - Jake Labelle

[DCG - Introducing Melbourne DCG by Allen and Friends](#) -

[DL - cont...\(16:00-17:55 PDT\)](#) - [CIRCO v2: Cisco Implant Raspberry Controlled Operations](#) - Emilio Couto

[DL - cont...\(16:00-17:55 PDT\)](#) - [Cotopaxi: IoT Protocols Security Testing Toolkit](#) - Jakub Botwicz

[ETV - cont...\(16:30-17:40 PDT\)](#) - [TechCongress](#) - Leisel Bogan

[ICS - cont...\(16:45-17:15 PDT\)](#) - [Industrial Cybersecurity in Mexico](#) - Octavio Fernandez,Victor Gomez

[IOT - IoT Honeypots and taming Rogue appliances](#) - Kat Fitzgerald

[LPV - Intro to high security locks and lockpicking](#) - N thing

[PHVW - cont...\(16:00-17:59 PDT\)](#) - [Advanced APT Hunting with Splunk](#) - Matt Toth,Robert Wagner

[RGV - cont...\(16:00-17:59 PDT\)](#) - [Outs, Forces, and Equivoque: A treatise on how Magicians speak](#) - Brandon Martinez

[RTV - cont...\(16:30-17:30 PDT\)](#) - [Indicators of Emulation: Extra Spicy Adversary Emulation](#) - Ch33r10,haydnjohnson

[RTV - \(17:45-18:45 PDT\)](#) - [Emulating an Adversary with Imperfect Intelligence](#) - Adam Pennington

[Return to Index - Locations Legend](#)

CNE - No Tech Talks -

CNE - Hacker Jeopardy -

CNE - (18:30-19:59 PDT) - [Film Festival: Project Immerse: A Deepfake Paranoid Thriller](#) -

ENT - tense future -

IOT - [Stepped on a Nail](#) - Matthew Byrdwell

RTV - cont...(17:45-18:45 PDT) - [Emulating an Adversary with Imperfect Intelligence](#) - Adam Pennington

[Return to Index - Locations Legend](#)

[CNE - cont...\(18:00-19:59 PDT\) - No Tech Talks](#) -

[CNE - cont...\(18:00-19:59 PDT\) - Hacker Jeopardy](#) -

[CNE - cont...\(18:30-19:59 PDT\) - Film Festival: Project Immerse: A Deepfake Paranoid Thriller](#) -

[ENT - Mica Husky](#) -

[FSL - Ask the EFF/Meet the EFA](#) - Abi Hassen,Alexis Hancock,Elliot,Emilie St-Pierre,Eva Galperin,Hannah Zhao,Kurt Opsahl,nash,Rory Mir,Tracy Rosenberg

[RTV - Automating Threat Hunting on the Dark Web and other nitty-gritty things](#) - Apurv Singh Gautam

[Return to Index - Locations Legend](#)

CNE - Whose Slide is It Anyway -

DC - Movie Stream - Lost World -

ENT - Dj St3rling -

RTV - (20:15-21:15 PDT) - [Bypassing in Mobile Network From Red-Team Points of View](#) - Ali Abdollahi

[Return to Index - Locations Legend](#)

CNE - cont...(20:00-21:59 PDT) - [Whose Slide is It Anyway](#) -

DC - cont...(20:00-21:59 PDT) - [Movie Stream - Lost World](#) -

ENT - [Skittish & Bus](#) -

PWDV - [Cracking at Extreme Scale: The Evolution of Hashstack \(Rebroadcast\)](#) - Jeremi M Gosney (epixoip)

RTV - cont...(20:15-21:15 PDT) - [Bypassing in Mobile Network From Red-Team Points of View](#) - Ali Abdollahi

RTV - (21:30-22:30 PDT) - [Sounds Legit: Why you shouldn't trust that speaker](#) - Luis Ángel Ramírez Mendoza (@larm182luis), Mauro Cáseres

[Return to Index - Locations Legend](#)

ENT - Miss Jackalope -

PWDV - Length 15 & No Change. Implementing NIST SP800-63B for real (Rebroadcast - Per Thorsheim

RTV - cont...(21:30-22:30 PDT) - [Sounds Legit: Why you shouldn't trust that speaker](#) - Luis Ángel Ramírez Mendoza (@Iarm182luis), Mauro Cáseres

RTV - (22:45-23:59 PDT) - [Weaponized XSS - Moving Beyond Alert\(1\)](#) - Ray Doyle

[Return to Index - Locations Legend](#)

ENT - Subxian -

PWDV - What the Shuck? Layered Hash Shucking (Rebroadcast) - Sam Croley (Chick3nman)

RTV - cont...(22:45-23:59 PDT) - Weaponized XSS - Moving Beyond Alert(1) - Ray Doyle

Sunday

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

Sunday - 01:00 PDT

[Return to Index](#) - [Locations Legend](#)

[PWDV - Practical PCFG Password Cracking \(Rebroadcast\)](#) - Matt Weir

[RTV - PatrOwl - Red flavour of SOC automation](#) - Nicolas MATTIOCCO

RTV - (02:15-03:15 PDT) - [Reviewing MS08-067, Illustration Of An Old Chapter](#) - Etizaz Mohsin

[Return to Index - Locations Legend](#)

[RTV - cont...\(02:15-03:15 PDT\) - Reviewing MS08-067, Illustration Of An Old Chapter](#) - Etizaz Mohsin

[RTV - \(03:30-04:30 PDT\) - RedTeamOps - Managing Red Team Infrastructure as a Red Teamer](#) - Mert Can Coşkun

[Return to Index - Locations Legend](#)

[RTV - cont...\(03:30-04:30 PDT\) - RedTeamOps - Managing Red Team Infrastructure as a Red Teamer](#) - Mert Can Coşkuner

[RTV - \(04:45-05:45 PDT\) - From Discovery to Disclosure](#) - Ibad Shah

[Return to Index - Locations Legend](#)

RTV - cont...(04:45-05:45 PDT) - [From Discovery to Disclosure](#) - Ibad Shah

[Return to Index - Locations Legend](#)

RTV - Hacking Zoom: a Hacker's Journey into Zoom Security - Mazin Ahmed

[Return to Index](#) - [Locations Legend](#)

RTV - (07:15-08:15 PDT) - [PWN The World](#) - Chris Kubecka

[Return to Index - Locations Legend](#)

[AEV - \(08:30-08:59 PDT\) - Hacking Airplane Air To Ground \(A2G\) Systems - Ali Abdollahi](#)

[RTV - cont...\(07:15-08:15 PDT\) - PWN The World - Chris Kubecka](#)

[RTV - \(08:30-09:30 PDT\) - Autonomous Security Analysis and Penetration Testing \(ASAP\) - Ankur Chowdhary](#)

[Return to Index - Locations Legend](#)

[AEV - Hacking Aerospace Cybersecurity Regulation](#) - Harley Geiger,Kaylin Trychon,Nicky Keeley

[AIV - Detecting hand-crafted social engineering emails with a bleeding-edge neural language model](#) - Younghoo Lee,Joshua Saxe

[ASV - Threagile - Agile Threat Modeling with Open-Source Tools from within Your IDE](#) - Christian Schneider

[BTWV1 - Introduction to Malware Analysis & Response \(MA&R\) \(Beginner\)](#) - Michael Wylie

[DC - \(09:30-09:59 PDT\) - Evil Printer: How to Hack Windows Machines with Printing Protocol](#) - Chuanda Ding,Zhipeng Huo

[HHV - Learn to Solder the BadgeBuddy Kit](#) - Joseph Long (hwbxr)

[PHVW - Bad Active Directory \(BAD\)](#) - Dhruv Verma,Michael Roberts,Xiang Wen Kuan

[RTV - cont...\(08:30-09:30 PDT\) - Autonomous Security Analysis and Penetration Testing \(ASAP\)](#) - Ankur Chowdhary

[RTV - \(09:45-10:45 PDT\) - Kubernetes Goat - Vulnerable by Design Kubernetes Cluster Environment](#) - Madhu Akula

[Return to Index](#) - [Locations Legend](#)

[AEV - Trust And Truth In Space Situational Awareness](#) - James Pavur
[AEV - \(10:30-10:59 PDT\) - 747 Walkthrough From A Hacker's Perspective](#) - Alex Lomas,Ken Munro
[AIV - Journal Club Live! Summoning Demons: The Pursuit of Exploitable Bugs in Machine Learning](#)
[ASV - Kubernetes Container Orchestration Security Assessment](#) - Ali Abdollahi
[ASV - The Elephant in the Room: Burnout](#) - Chloé Messdaghi
[BCV - Welcome Note](#)
[BCV - Modeling systematic threat: testing on mainnet fork](#) - Martinet Lee
[BHV - DAY3 KEYNOTE: Why is Security Hard?](#) - Seth Carmody
[BHV - \(10:30-10:59 PDT\) - Infodemic: Threat models for patient communities on social networks](#) - Andrea Downing
[BTVW1 - cont...\(09:00-10:30 PDT\) - Introduction to Malware Analysis & Response \(MA&R\) \(Beginner\)](#) - Michael Wylie
[BTVW2 - \(10:30-11:59 PDT\) - Incident Response and the ATT&CK Matrix \(Beginner\)](#) - Sam Bowne
[CHV - Hacking Ludicrous Mode on a Tesla \(moar power!!\)](#) - Patrick Kiley
[CPV - \(10:30-10:59 PDT\) - European regulatory trends for Artificial Intelligence: same impact on US as GDPR?](#) - Julia Reinhardt
[DC - \(10:30-10:59 PDT\) - Bytes In Disguise](#) - Jesse Michael,Mickey Shkatov
[DL - redlure](#) - Matthew Creel
[DL - MalConfScan with Cuckoo](#) - Tomoaki Tani,Shusei Tomonaga
[ETV - Blackmail, Extortion and the Ethics of Disclosure](#) - Michael Antonino
[HHV - Meetup: Sourcing Parts](#) - bombnav
[HRV - The K0BAK Rover Van](#) -
[LPV - Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
[MOV - Keynote: Monero: Sound Money Safe Mode](#) - Dr. Daniel Kim
[PAYV - PoS Terminal Security Uncovered](#) - Aleksei Stennikov
[PHVW - cont...\(09:00-12:59 PDT\) - Bad Active Directory \(BAD\)](#) - Dhruv Verma,Michael Roberts,Xiang Wen Kuan
[RTV - cont...\(09:45-10:45 PDT\) - Kubernetes Goat - Vulnerable by Design Kubernetes Cluster Environment](#) - Madhu Akula

[Return to Index - Locations Legend](#)

- [AEV - Critical Aerospace Cybersecurity: How Hacking And Designing Aerospace Systems Is Changing](#) - Lawrence Rowell,Nathalie Feyt,Yannick Le Ray
- [ASV - cont...\(10:00-11:59 PDT\) - Kubernetes Container Orchestration Security Assessment](#) - Ali Abdollahi
- [ASV - A Heaven for Hackers: Breaking a Web Security Virtual Appliances](#) - Mehmet D. Ince
- [BCV - Building a Microcontroller Bitcoin Address Generator](#) - chaintuts,Josh McIntyre
- [BHV - How Independent Security Researchers work with Medical Device Manufacturers - The Bad, The Ugly & The Great \(BUG\)](#) - Kyle Erickson,Natali,Peter,Veronica
- [BTWV2 - cont...\(10:30-11:59 PDT\) - Incident Response and the ATT&CK Matrix \(Beginner\)](#) - Sam Bowne
- [CLV - Cloud host base strategy by staging defensive tools for Threat Hunting and Forensics](#) - Michael Mimo
- [CLV - \(11:45-12:30 PDT\) - Remediation Framework - Auto respond to AWS nightmares.](#) - Sahir Khan,Justin Paglierani
- [CPV - Fear, Uncertainty, and Doubt about Human Microchip Implants](#) - Zhanna Malekos Smith
- [CPV - \(11:30-11:59 PDT\) - What if we had TLS for phone numbers? An introduction to SHAKEN/STIR](#) - Kelley Robinson
- [DC - \(11:30-11:59 PDT\) - Only takes a Spark - Popping a shell on a 1000 nodes](#) - ayoul3
- [DL - cont...\(10:00-11:50 PDT\) - redlure](#) - Matthew Creel
- [DL - cont...\(10:00-11:50 PDT\) - MalConfScan with Cuckoo](#) - Tomoaki Tani,Shusei Tomonaga
- [HHV - \(11:30-12:30 PDT\) - HackerBox 0057 Build Session](#) - Joseph Long (hwbxr)
- [HRV - cont...\(10:00-11:30 PDT\) - The K0BAK Rover Van](#) -
- [HTS - Hack the SeaPod](#) - Fathom5
- [LBV - Bypass 101 + Q&A](#)
- [LPV - Safecracking for Everyone!](#) - Jared Dygert
- [MOV - cont...\(10:00-11:30 PDT\) - Keynote: Monero: Sound Money Safe Mode](#) - Dr. Daniel Kim
- [PAYV - Architecting Modern Payment Gateways in .Net core with Azure](#) - Menaka BaskerPillai
- [PHVT - Packet Acquisition: Building the Haystack](#) - Chris Abella,Pete Anderson
- [PHVW - cont...\(09:00-12:59 PDT\) - Bad Active Directory \(BAD\)](#) - Dhruv Verma,Michael Roberts,Xiang Wen Kuan
- [RTV - Breaking the Attack Chain](#) - Corey Ham,Matt Eidelberg

[Return to Index - Locations Legend](#)

[AEV - Cybersecurity Lessons Learned From Human Spaceflight](#) - Pam Melroy
[ASV - Secure Your Code — Injections and Logging](#) - Philipp Krenn
[BCV - exploit insecure crypto wallet](#) - Minzhi He, peiyu wang
[BCV - \(12:40-12:59 PDT\) - Closing Note](#)
[BHV - \(12:30-12:59 PDT\) - How to Grow a Brain in a Jar - Neuroengineering 101](#) - Jack
[BTWV1 - Deploying Pi-hole: More Than an Ad Blocker \(Beginner\)](#) - Ben Hughes
[CLV - cont...\(11:45-12:30 PDT\) - Remediation Framework - Auto respond to AWS nightmares.](#) - Sahir Khan, Justin Paglierani
[CLV - \(12:30-13:30 PDT\) - Cloud-Native Attack Detection and Simulation.](#) - Nick Jones
[CPV - Workshop: Let's Talk About Abusability Testing](#) - Avi Zajac, Franchesca Spektor, Ji Su Yoo, Nicole Chi
[DL - Carnivore \(Microsoft External Attack Tool\)](#) - Chris Nevin
[DL - Starkiller](#) -
[ETV - How to Start a Movement: Hackers Edition](#) - Chloé Messdaghi
[HHV - cont...\(11:30-12:30 PDT\) - HackerBox 0057 Build Session](#) - Joseph Long (hwbxr)
[HHV - \(12:30-12:59 PDT\) - Meetup: Wearables](#) - ShortTie
[LBV - cont...\(11:00-12:30 PDT\) - Bypass 101 + Q&A](#)
[LPV - Intro to Lockpicking](#) - The Open Organisation Of Lockpickers
[MOV - You're not the money printer, or why we need to separate coinbase rings](#) - sgp
[PHVW - cont...\(09:00-12:59 PDT\) - Bad Active Directory \(BAD\)](#) - Dhruv Verma, Michael Roberts, Xiang Wen Kuan
[RGV - Rogues adventure & the intervillage badge](#) - Monero Village Team, Rogues Village Team
[RTV - \(12:15-13:15 PDT\) - Hashes; Smothered, Covered, and Scattered: Modern Password Cracking as a Methodology](#) - Lee Wangenheim
[WLV - Ghosting the PACS-man: New Tools and Techniques](#) - Iceman, Omikron

[Return to Index - Locations Legend](#)

- [AEV - Dissecting Wireless Privacy In Aviation](#) - Martin Strohmeier
- [AEV - \(13:30-13:59 PDT\) - Breakdown Of The FAA's Privacy ICAO Address Program](#) - Gui Michel
- [AIV - Faults in our Pi Stars: Security Issues and Challenges in Deep Reinforcement Learning](#) - Vahid Behzadan
- [ASV - Running an appsec program with open source projects](#) - Vandana Verma Sehgal
- [BHV - \(13:15-13:45 PDT\) - The Underestimated Threat Vector: Homogeneity](#) - Vidya Murthy
- [BHV - \(13:30-14:30 PDT\) - Making Next Generation Drugs at Home](#) - Mixael Swan Laufer
- [BTWV1 - cont...\(12:00-13:30 PDT\) - Deploying Pi-hole: More Than an Ad Blocker \(Beginner\)](#) - Ben Hughes
- [BTWV2 - \(13:30-14:59 PDT\) - Cloud Security Monitoring on a Dime Store Budget \(Beginner\)](#) - Wes Lambert
- [CLV - cont...\(12:30-13:30 PDT\) - Cloud-Native Attack Detection and Simulation.](#) - Nick Jones
- [CLV - \(13:30-13:50 PDT\) - Closing Note](#) -
- [CPV - File Encryption For Actual Humans](#) - David Kane-Parry
- [DL - cont...\(12:00-13:50 PDT\) - Carnivore \(Microsoft External Attack Tool\)](#) - Chris Nevin
- [DL - cont...\(12:00-13:50 PDT\) - Starkiller](#) -
- [HHV - Importing vector graphics in to EagleCAD](#) -
- [HRV - APRS: Automatic Packet Reporting System Demo](#) -
- [LPV - Keystone to the Kingdom](#) - Austin Marck
- [MOV - Locha Mesh: Monero off-the-grid](#) - Randy Brito
- [MOV - \(13:30-14:30 PDT\) - Badge Clinic](#) - Michael Schloh von Bennewitz
- [RGV - cont...\(12:00-13:59 PDT\) - Rogues adventure & the intervillage badge](#) - Monero Village Team,Rogues Village Team
- [RTV - cont...\(12:15-13:15 PDT\) - Hashes; Smothered, Covered, and Scattered: Modern Password Cracking as a Methodology](#) - Lee Wangenheim
- [RTV - \(13:30-14:30 PDT\) - You're Adversary Within - The Golden Age of Insider Threats](#) - Adam Mashinchi

[Return to Index](#) - [Locations Legend](#)

[AEV](#) - [Hack-A-Sat Closing Segment](#) -

[AIV](#) - [Ethics & Bias Panel](#)

[BHV](#) - [cont...\(13:30-14:30 PDT\)](#) - [Making Next Generation Drugs at Home](#) - [Mixael Swan Laufer](#)

[BHV](#) - [Open Ventilator Remote Monitoring Project](#) -

[BHV](#) - [\(14:45-16:45 PDT\)](#) - [Securing Your Medical Device Network on a Shoestring Budget](#)

[BTWV2](#) - [cont...\(13:30-14:59 PDT\)](#) - [Cloud Security Monitoring on a Dime Store Budget \(Beginner\)](#) - [Wes Lambert](#)

[DC](#) - [\(14:30-14:59 PDT\)](#) - [Beyond Root: Custom Firmware for Embedded Mobile Chipsets](#) - [Christopher Wade](#)

[ETV](#) - [Open Live Chat for all Speakers or another talk on Ethics of Moderation](#) - [Ethics Village Staff](#)

[HHV](#) - [Learn to Solder the BadgeBuddy Kit](#) - [Joseph Long \(hwbxr\)](#)

[HRV](#) - [\(14:30-14:45 PDT\)](#) - [Village Closing Commentary](#) -

[LBV](#) - [DIY Bypass Tool Workshop + Q&A](#)

[LPV](#) - [\(14:15-14:45 PDT\)](#) - [Intro to Lockpicking](#) - [The Open Organisation Of Lockpickers](#)

[MOV](#) - [cont...\(13:30-14:30 PDT\)](#) - [Badge Clinic](#) - [Michael Schloh von Bennewitz](#)

[RTV](#) - [cont...\(13:30-14:30 PDT\)](#) - [You're Adversary Within - The Golden Age of Insider Threats](#) - [Adam Mashinchi](#)

Sunday - 15:00 PDT

[Return to Index - Locations Legend](#)

[AEV - Cybersecurity Meets Aviation Regulation](#) - Aaron Cornelius, Tim Brom

[AIV - \(15:30-15:59 PDT\) - Closing Remarks](#)

[BHV - cont...\(14:45-16:45 PDT\) - Securing Your Medical Device Network on a Shoestring Budget](#)

[BTWV1 - Azure AD Logs for the Blue Team \(Intermediate\)](#) - Mark Morowczynski

[DC - \(15:30-15:59 PDT\) - Practical VoIP/UC Hacking Using Mr.SIP: SIP-Based Audit & Attack Tool](#) - Ismail Melih Tas, Kubilay Ahmet Kucuk

[DCG - DEF CON Groups Panel](#) - Brent White / B1TK1LL3R, Casey Bourbonnais / ADAM_915, Jayson E. Street, April C Wright

[HRV - Ham Radio USA License Exams \(Sunday\)](#) -

[LBV - cont...\(14:00-15:30 PDT\) - DIY Bypass Tool Workshop + Q&A](#)

[LBV - \(15:30-16:59 PDT\) - General Q&A / Drop-in and Chat](#)

[LPV - How I defeated the Western Electric 30c](#) - N thing

[MOV - \(15:30-15:59 PDT\) - Closing talk](#) - rehr

[RTV - Have my keys been pwned? - API Edition](#) - José Hernandez, Rod Soto

[Return to Index - Locations Legend](#)

[AEV - What I Learned Trying To Hack A 737](#) - Karl Koscher

[BHV](#) - cont...(14:45-16:45 PDT) - Securing Your Medical Device Network on a Shoestring Budget

[BTVT1](#) - Blue Team Village Closing Ceremony

[DC](#) - (16:30-16:59 PDT) - [Lateral Movement and Privilege Escalation in GCP; Compromise any Organization Without](#)

[Dropping an Implant](#) - Allison Donovan,Dylan Ayrey

[HRV](#) - cont...(15:00-17:59 PDT) - [Ham Radio USA License Exams \(Sunday\)](#) -

[LBV](#) - cont...(15:30-16:59 PDT) - General Q&A / Drop-in and Chat

[LPV](#) - (16:15-16:45 PDT) - [Intro to Lockpicking](#) - The Open Organisation Of Lockpickers

[RTV](#) - [Red Team Village Closing Ceremony and Announcement of Winners of CTF and CyberWraith](#) - Joseph

Młodzianowski (cedoXx),Omar r

[Return to Index - Locations Legend](#)

[DC - Closing Ceremonies - The Dark Tangent](#)

[HRV - cont...\(15:00-17:59 PDT\) - Ham Radio USA License Exams \(Sunday\) -](#)

Speaker List

Anders Fogh
Anders Fogh
Özkan Mustafa Akkus
Aaron Cornelius
Aaron Soto
Abi Hassen
ac0rn
Adam Mashinchi
Adam Mashinchi
Adam Pennington
Adama Ibrahim
Aditi Joshi
AI Village Journal Club
AI Village Organizers
Ajin Abraham
Akira Takahashi
Al Burke
Aleksei Stennikov
Alex Lomas
Alex Lomas
Alex Lomas
Alex Zaheer
Alexander Korotin
Alexandre Beaulieu
Alexandre Sieira
Alexis Hancock
Ali Abdollahi
Ali Abdollahi
Ali Abdollahi
Allan Stojanovic
Allan Tart
Allen Baranov
Allie Barnes
Allie Hansen
Allie Mellen
Allison Donovan
Alvaro Folgado Rueda
Alvaro Munoz
Alyssa Miller
Amèlie Koran
Amber Graner
Amelie Koran
Amit Elazari
Amy Abernethy
Anahit Tarkhanyan
Andrea Downing
Andrea Matwyshyn
Andrew Chu
Andrew Tierney
Ankur Chowdhary
Anna McAbee

Anthony DiFranco
Anthony Rose
April C Wright
Apurv Singh Gautam
Ariel Schön
Arkadiy Litvinenko
Ash Luft
atlas Of d00m
Austin Marck
Austin Marck
Austin Scott
Avi Zajac
Avi Zajac
Avi Zajac
ayoul3
Barak Schoster
Barak Sternberg
Ben Bornholm
Ben Bornholm
Ben Brook
Ben Dubov
Ben Gardiner
Ben Gardiner
Ben Hughes
Ben Hughes
Benjamin Hovland
Besim Altinok
Bianca Lewis
Bill Demirkapi
Bill Graydon
Bob Wheeler
bombnav
bombnav
Brandon Bailey
Brandon Martinez
Brenda So
Brent Stone
Brent White / B1TK1LL3R
Brig. Gen. William Hartman
Bryson Bort
Bryson Bort
Bryson Bort
C. Nadal
C8 (John Hammond)
Caleb Gardner
Can Demirel
Cannibal
Casey Bourbonnais / ADAM_915
Casey John Ellis
Casey John Ellis
Cathy Gellis
Cecilie Wian
cemaxecuter
Ch33r10
Ch33r10

chaintuts
Chet Hosmer
Chloé Messdaghi
Chloé Messdaghi
Chloé Messdaghi
Chloé Messdaghi
Chloé Messdaghi
Chris Abella
Chris Gammell
Chris Krebs
Chris Krebs
Chris Kubecka
Chris Kubecka
Chris Nevin
Chris Nevin
Chris Pimlott
Chris Poore
Chris Wysopal
Christian “quaddi Dameff
Christian “quaddi Dameff
Christian Schneider
Christopher Cottrell
Christopher Wade
Chuanda Ding
Colin Cantrell
Colin Estep
comathematician
Comm. Geoffrey Starks
Comm. Rohit Chopra
Connor Morley
Cooper Quintin
Cordero Alexander Delgadillo
Corey Ham
corvusactual
CRob
CRob
Cynthia Kaiser
d1dymu5
Dan Kimmage
Dan Salloum
Dani Goland
Dani
Daniel Gruss
Daniel Gruss
Daniel Miessler
Daniel Roy
Daniel Roy
Daniel Ward
David Bernal Michelena
David Imbordino
David J. Bianco
David Kane-Parry
David Robinson
David Sopas

David Waldrop
Dena Medelsohn
Denise Giusto Bilic
Derrick (CanBusDutch)
Devabhaktuni Srikrishna
Dewank Pant
Dhruv Verma
Diane Janosek
Diane Vavrichek
Diego F. Aranha
Dor Yardeni
Dr Lorenz Adlung
Dr Mohammed Aamir Ali
Dr Steven J. Murdoch
Dr Will Roper
Dr. Catherine Ullman
Dr. Daniel Kim
Dr. Daniel Kim
Dr. Daniel Kim
Dr. Francisco "ArticMine" Cabañas
Dr. Gary Kessler
Dr. Khatuna Mshvidobadze
Dr. Mike Rushanan
Dr. Nina Kollars
Dr. Sarah Blossom Ware
drhyrum
Dylan Ayrey
Dylan The Magician
Ece Gumusel
Eduardo Arriols
Eirick Lurass
Eivind Arvesen
Elie Bursztein
Elizabeth Biddlecome
Elliot
Emilie St-Pierre
Emilio Couto
Emilio Couto
Emily Stamm
Enrico Pozzobon
Erdener Uyan
Eric Escobar
Eric Escobar
erickgalinkin
Erik Hunstad
Erin Miller
Ethics Village Staff
Etizaz Mohsin
Eva Galperin
Evan Anderson
EvilMog
EvilMog
Eyal Itkin
F. Novaes
Fabian Landis

Farith Pérez Sáez
Farith Pérez Sáez
Farith Perez
Fathom5
Federico Lucifredi
Federico Lucifredi
Feng Xiao
Forrest Fuqua
Forrest Senti
Forrest Senti
Fran Ramirez
Francesco Gringoli
Franchesca Spektor
Franchesca Spektor
Franchesca Spektor
Fredrick "Flee" Lee
FreyXin
Gökberk Gülgün
Gabriel Ryan
Gal Zror
Garrett Enoch
Gokul Alex
Graham Bleaney
Grant Romundt
Gregg Horton
GTKlondike
Gui Michel
Guillermo Buendia
hackingdave
Hadrien Barral
Hank Leininger
Hank Leininger
Hannah Zhao
Hanno Böck
Harley Geiger
Harri Hursti
Harshad Sathaye
Harshad Sathaye
haydnjohnson
Holger Unterbrink
Huajiang "Kevin2600" Chen
I. Shaheem
Ibad Shah
Iceman
idk
Infenet
Infenet
Infenet
Infenet
Irvin Lemus
Ismail Melih Tas
J. DeBlois
Jack Baker
Jack Cable
Jack Cable

Jack McDowell
Jack Mott
Jack
Jackie Speier
Jaime
Jaime
Jaime
Jake “Hubbl3 Krasnov
Jake Labelle
Jake Smith
Jakub Botwicz
James Harrison
James Pavur
James Pavur
Jared Dygert
Jarrod Overson
Jason Haddix
Jason Williams
Javad Dadgar
Javier F. Patiño García
Jay Angus
Jayson E. Street
Jeff “r3plicant Tully
Jeff “r3plicant Tully
Jeff Troy
Jeff Troy
Jen Ellis
Jen Goldsack
Jenai Marinkovic
Jenko Hwong
Jeremi M Gosney (epixoip)
Jeremi M Gosney (epixoip)
Jesse Michael
Jessica Wilkerson
Jeswin Mathai
Ji Su Yoo
Ji Su Yoo
Ji Su Yoo
Jiska Classen
João Morais
Jody Westby
Joe Billingsley
Joe Schottman
Joe Schottman
Joe Slowik
Joe Slowik
John Craig
John Felker
John Odum
John the Greek
Jonathan Helmus
Jonathan Stines
Jorge Orchilles
Jorge Orchilles
José Hernandez

Jose Miguel Gómez-Casero Marichal

Jose Rodriguez

Joseph Long (hwbxr)

Joseph Młodzianowski (cedoXx)

Joseph Młodzianowski (cedoXx)

Joseph Młodzianowski (cedoXx)

Joseph Młodzianowski (cedoXx)

Josh Marks

Josh McIntyre

Josh O'Connor

Josh Stroschein

Josh

Joshua Maddux

Joshua Saxe

Juan Francisco

Julia Reinhardt

Julian Suleder

JunWei Song

Justin Hutchens ("Hutch")

Justin Paglierani

Kürşat Oğuzhan Akıncı

Kaitlyn Handleman

Kamel Ghali

Kamel Ghali

Kamel Ghali

Kamel Ghali

Karl Koscher

Kat Fitzgerald

Kat Fitzgerald

Kate Venable

Katelyn Bowden

Katie Doroschak

Katie Noble

Katie Noble

Katie Noble

Kaustubh Padwad

Kaylin Trychon

Kelley Robinson

Kelley Robinson

Ken Munro

Ken Munro

kennwhite

Kevin Leffew

Kim Wyman

Kimber Dowsett

Kirsten Renner

Kris Jones

Kris Rides

Kris Rides

Kubilay Ahmet Kucuk
KunYu Chen
Kurt Opsahl
Kyle Benac (aka @B3nac)
Kyle Erickson
Ladislav B
Larry Lewis
Laurin Weissinger
Lawrence Rowell
Lee Wangenheim
Leigh-Anne Galloway
Leisel Bogan
Lennart Koopmann
Leron Gray
Levi
Lisa Bradley
Lisa Bradley
Litmoose
Litmoose
Liz Popiak
Liz Wharton
Imeyerov
Louis Nyffenegger
Lucia Savage
Luis Ángel Ramírez Mendoza (@larm182luis)
Luis Ángel Ramírez Mendoza (@larm182luis)
Luis Ángel Ramírez Mendoza (@larm182luis)
M. DeBlois
M. Tibouchi
Mário Areias
Maddie Stone
Madhu Akula
Maggie MacAlpine
Mangatas Tondang
Mansi Sheth
Mansi Sheth
Marcelo Sacchetin
Marie
Marina Krotofil
Maritza Johnson
Mark Bereza
Mark Morowczynski
Mark Nesbitt
Marleigh Farlow
Marten Mickos
Martin Abbatemarco
Martin Strohmeier
Martinet Lee
Master Chen
Matt Blaze
Matt Cheung
Matt Duren
Matt Eidelberg
Matt Gaffney
Matt Luongo

Matt Murray
Matt Smith
Matt Toth
Matt Weir
Matt Weir
Matthew Byrdwell
Matthew Creel
Matthew Creel
Matthew Gaffney
Matthew Masterson
Mattie Gullixson
Mattie Gullixson
Mauricio Velazco
Mauro Cáseres
Mauro Cáseres
Mauro Cáseres
Mauro Cáseres
Mauro Cáseres
Mazin Ahmed
Megan DeBlois
Mehmet D. Ince
Menaka BaskerPillai
Mert Can Coşkuner
Mert Can Coşkuner
Michael A. Specter
Michael Antonino
Michael Mimo
Michael Roberts
Michael Schloh von Bennewitz
Michael Schloh von Bennewitz
Michael Schloh von Bennewitz
Michael Schloh von Bennewitz
Michael Stay
Michael Vanguardia
Michael Wylie
Michael Wylie
Michael Wylie
Michael Wylie
Michael Wylie
Michelle Holko
Mickey Shkatov
Mike Cohen
Mike Lemley
Mike Murray
Mike Raggo
Minga
Minga
Mintynet
Mintynet
Minzhi He
Mitchell Parker
Mixæl Swan Laufer
Mohammad-Reza Zamiri
Mohit Gupta
Mohsan Farid

Monero Village Team
Moshe Kol
Muteki
N thing
N thing
Nadav Erez
NahamSec
Nahid Farhady
Nahid Farhady
Nailah Mims
Najla Lindsay
nash
Natali
Nate DeNicola
Nathalie Feyt
Neil M
Netspooky
Nick Jones
Nicky Keeley
Nicolas MATTIOCCO
Nicole Chi
Nicole Chi
Nicole Chi
Nils Weiss
Nimit Sawhney
Nimrod Kor
Nina Alli
Nishant Sharma
Nishant Sharma
Noa Novogroder
nohackme
Octavio Fernandez
Oleksandr Mirosh
Olivier Bilodeau
Olivier Bilodeau
Omar r
Omar r
Omar r
Omar Santos
Omar Santos
Omar Santos
Omescan
Omikron
Otis
Pablo Breuer
Pablo Gonzalez
PacketSqueezins
Pam Melroy
Parker Wiksell
Parsia Hakimian
Password Village Staff
Password Village Staff
Password Village Staff
Password Village Staff
Password Village Staff

Password Village Staff

Patrick Kiley

Patrick Kiley

Patrick Kiley

Patrick Wardle

Paul Amar

Paul Marrapese

Paul Melson

Paulo Silva

Pedro Umbelino

peiyu wang

Peleg Hadar

Per Thorsheim

Per Thorsheim

Pete Anderson

Pete Cooper

Pete Cooper

Pete Keenan

Pete Radloff

Peter Kacherginsky

Peter Kacherginsky

Peter

Petros Koutroumpis

Philipp Krenn

Phillip Marlow

Phillip Marlow

Phillip Wylie

Plug

Plug

Plug

Poming Lee

Porter Adams

Preston Thomas

R. Jason Cronk

Rémi Géraud-Stewart

Rachel Bozeman

Rachel Lamp

Radu Motspan

Rand0h

Randy Brito

Randy Talley (CISA)

Ray Doyle

rehr

rehr

rehr

rehr

rehr

rehr

rehr

Reza Dorosti

Riana Pfeifferkorn

Rick Hansen

Rik van Duijn

Rim Boujnah

Robert Leale (CarFuCar)

Robert Leale (CarFuCar)
Robert Leale (CarFuCar)
Robert Wagner
Roberto Rodriguez
Roberto Rodriguez
Rod Soto
Rogues Village Team
Rogues Village Team
Roman Vitkovitsky
Ron Stoner
Ron Wyden
Rory Mir
Roy Wattanasin
Russell Mosley
Ruth Barbacil
Ryan Elkins
Ryan Rubin
Ryan Slama
Ryoichi Teramura
Ryosuke Uematsu
Sahir Khan
Sajal Thomas
Sam Bowne
Sam Bowne
Sam Bowne
Sam Croley (Chick3nman)
Sam Croley (Chick3nman)
Samir
Samuel Gasparro
Sang-Oun Lee
Sanjana Sarda
Sarang
Scoubi
Scoubi
Sean Metcalf
Sebastian Banescu
Serkan Temel
Seth Carmody
Setu Parimi
Seungjoo
sgp
Shay Nehmad
Shlomi Oberman
Shogo Nakao
ShortTie
ShortTie
ShortTie
ShortTie
Shruti Lohani
Shusei Tomonaga
Sidd Gejji
Simon Weckert
Slava Makkaveev
Spencer Cureton
Spencer Gietzen

Stanislas Molveau
Stephanie Singer
Stephen Gerling
Steve Newell
Steven Bernstein
Suhyeon Lee
Susan Greenhalgh
Suzanne Schwartz
Tanner Barnes (aka @_StaticFlow_)
Tatsuya Katsuhara
Teejay
Tejaswa Rastogi
The Dark Tangent
The Dark Tangent
The Open Organisation Of Lockpickers
The Red Dragon
TheDrPinky
Thomas Hayes
Tim Brom
Tim Doomsday
Tim Wadhwa-Brown
Tim Yardley
TimDotZero
Timur Yunusov
Tod Beardsley
Tom
Tomer Bar
Tomoaki Tani
Tony M Lambert
Tony Virelli
Tracy Rosenberg
Travis LeBlanc
Travis Palmer
Trevor Stevado t1v0
Trey Keown
Troy Brown
ttheveii0x
Tyler Boykin
Uri Rivner
Utku Sen
Utku Sen
Vahid Behzadan
Valentina Palacín
Vandana Verma Sehgal

Vandana Verma Sehgal
Vee Schmitt
Veronica
Veronica
Vic Harkness
Victor Fang
Victor Gomez
Vidya Murthy
Vidya Murthy
Vincent “Vinnybod Rose
Viral Maniar
Vyrus
Walter Cuestas
Wes Lambert
Wes Lambert
Wesley Neelen
Whitney Champion
wytshadow
Xavier Ashe
Xavier Ashe
Xiang Wen Kuan
Y. Yarom
Yamila Levalle
Yannick Le Ray
Yong-Bee
Younghoo Lee
Yuchao (Alex) Zhang
Yusuf Henriques
Z. Anderson
Zach Singleton
zeefeene
zh4ck
Zhanna Malekos Smith
Zhipeng Huo

Talk List

"SECRETS ARE LIES, SHARING IS CARING, PRIVACY IS THEFT." - A Dive into Privacy Preserving Machine Learning - AIV

10,000 Dependencies Under The Sea: Exploring and Securing Open source dependencies - ASV

21 Jump Server: Going Bastionless in the Cloud - CLV

2FA in 2020 and Beyond - ASV

40,000 Leagues UUV Death Match - HTS

5 Quick Wins for Improving your ICS Cybersecurity Posture - ICS

50 Shades of Sudo Abuse - RTV

7 Phases of Smart Contract Hacking - BCV

747 Walkthrough From A Hacker's Perspective - AEV

A Basic Ham Station Setup - HRV

A Decade After Stuxnet's Printer Vulnerability: Printing is still the Stairway to Heaven - DC

A Deeper Dive Into ILS And ADS-B Spoofing - AEV

A Hacker's guide to reducing side-channel attack surfaces using deep-learning - DC

A Heaven for Hackers: Breaking a Web Security Virtual Appliances - ASV

A Lawyer's Reflections on Elections - VMV

A N00b's Intro to Building Your Own Lab (Beginner) - BTWV2

A Panel with the Feds on Election Security - VMV

A Policy Approach to Resolving Cybersecurity Problems in the Election Process - VMV

A View From The Cockpit: Exploring Pilot Reactions To Attacks On Avionic Systems - AEV

Abusing P2P to Hack 3 Million Cameras: Ain't Nobody Got Time for NAT - DC

Acid T - ENT

Adding new features by manipulating CAN bus - CHV

Advanced APT Hunting with Splunk - PHVW

Advancing Medical Device Security – How collaboration between providers, manufacturers, and pen testers is advancing what's possible with security. - BHV

Aerospace Village Badge - AEV

AI vs. Airplanes and IT-Security: What Security Regulations Teach Us About AI Governance - AIV

All Aboard the CAN Bus... or Motorcycle - CHV

All of the threats: Intelligence, modelling and hunting through an ATT&CKers lens - RTV

AMA w/@hackingdave & @kennwhite - POV

AMA w/ Policymakers - POV

Ambly, the Smart Darknet Spider - RCV

An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology (Beginner) - BTWV2

An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology (Beginner) - BTWV2

Analysis of the Attack Data Collected During Mobile Voting Pilots - VMV

Android Application Exploitation - RTV

Android Bug Foraging - ASV

Android Malware Adventures - RTV

API (in)Security TOP 10: Guided tour to the Wild Wild World of APIs - ASV

Applied Ca\$h Eviction through ATM Exploitation - DC

Applying Pysa to Identify Python Security Vulnerabilities - ASV

APRS: Automatic Packet Reporting System Demo - HRV

APTs <3 PowerShell and Why You Should Too - RTV

Architecting Modern Payment Gateways in .Net core with Azure - PAYV

Ask the EFF/Meet the EFA - FSL

Assembling VULNtron: 4 CVEs that Turn a Teleconference Robot into a Spy - IOT

Attacking and Defending Blockchain Nodes - BCV

Attacking Flight Management Systems: This Is Your Captain Speaking, We Have A Small Problem! - AEV

Attacking the Helmsman - CLV

ATTPwn: Adversarial Emulation and Offensive Techniques Collaborative Project - RTV

Automating Threat Hunting on the Dark Web and other nitty-gritty things - RTV

Automotive Ethernet for the rest of us - CHV
Automotive Ethernet for the rest of us - CHV
Automotive In-Vehicle Networks - CHV
Automotive In-Vehicle Networks - CHV
Autonomous Security Analysis and Penetration Testing (ASAP) - RTV
Azure AD Logs for the Blue Team (Intermediate) - BTWV1
Baby's First 100 MLSec Words - AIV
Back to the future: Computer science and systems biology - RTV
Bad Active Directory (BAD) - PHVW
Badge Clinic - MOV
Badge Clinic - MOV
Basic OSINT: Mining Personal Data - DCG
Be Like Water: What Bruce Lee Can Teach Us About AppSec - ASV
Before J1939: A J1708/J1587 Protocol Decoder - CHV
Beyond Root: Custom Firmware for Embedded Mobile Chipsets - DC
Blackmail, Extortion and the Ethics of Disclosure - ETV
Blockchain for Cyber Defense: Will it be as good as you think? - BCV
Blue Team Village & Red Team Village Panel - BTVT1
Bluetooth Security in Automotive - CHV
Bluetooth Security in Automotive - CHV
Bobby Pins, More Effective Than Lockpicks? - LPV
Breakdown Of The FAA's Privacy ICAO Address Program - AEV
Breaking the Attack Chain - RTV
Build a Raspberry AIS - HTS
Building a Microcontroller Bitcoin Address Generator - BCV
Building a Physical Testbed for Blackstart Restoration under Cyber Fire - ICS
Building BLUESPAWN: An Open-Source, Active Defense & EDR Software (Intermediate) - BTVT1
Building Connections Across The Aviation Ecosystem - AEV
Building Teams in the New Normal - CRV
Burnout is real - RCV
But I Still Need A Job! - CRV
Bypassing Biometric Systems with 3D Printing and Enhanced Grease Attacks - DC
Bypassing in Mobile Network From Red-Team Points of View - RTV
Bytes In Disguise - DC
CAN be super secure: Bit Smashing FTW - CHV
Can't Touch This: Detecting Lateral Movement in Zero-Touch Environments - CLV
Can't Touch This: Detecting Lateral Movement in Zero-Touch Environments - ASV
Car (to Cloud) Talk: Using MQTT for Car Hacking - CHV
Car (to Cloud) Talk: Using MQTT for Car Hacking - CHV
Carnivore (Microsoft External Attack Tool) - DL
Carnivore (Microsoft External Attack Tool) - DL
Catch Me if You Can - RTV
Chairman Benjamin Hovland, US Election Assistance Commission - VMV
Checklist For Aviation Vulnerability Disclosure: Don't Go It Alone - AEV
Chinese Military Laboratory Mission + COVID-19 - BHV
ChupaCarBrah: Open Source Hardware and Software for Interacting with your Vehicle CAN Bus - CHV
CIRCO v2: Cisco Implant Raspberry Controlled Operations - DL
CIRCO v2: Cisco Implant Raspberry Controlled Operations - DL
Closing Ceremonies - DC
Closing Note - CLV
Closing talk - MOV
Cloud Frontier - CLV
Cloud host base strategy by staging defensive tools for Threat Hunting and Forensics - CLV
Cloud Security Monitoring on a Dime Store Budget (Beginner) - BTWV2
Cloud Village CTF - CLV

Cloud-Native Attack Detection and Simulation. - CLV
Cluster fuzz! - CHV
Cluster fuzz! - CHV
CMAP: Open Source Vehicle Services Mapping Tool for noobs - CHV
Combining notebooks, datasets, and cloud for the ultimate automation factory - RTV
Confessions of an Offensive ICS Cyber Security Researcher - ICS
Cons and Careers - CRV
Cotopaxi: IoT Protocols Security Testing Toolkit - DL
COVID 1984_ Propaganda and Surveillance during a Pandemic - RCV
Cracking at Extreme Scale: The Evolution of Hashstack (Rebroadcast) - PWDV
Cracking at Extreme Scale: The Evolution of Hashstack - PWDV
Creating a decentralized storage for Kubernetes with Tardigrade and Velero - BCV
Critical Aerospace Cybersecurity: How Hacking And Designing Aerospace Systems Is Changing - AEV
Cryptocurrencies have superusers? - BCV
Cybersecurity informed consent for medical devices - BHV
Cybersecurity Lessons Learned From Human Spaceflight - AEV
Cybersecurity Meets Aviation Regulation - AEV
Cypher for Defenders: Leveraging Bloodhound Data Beyond the UI (Intermediate) - BTWV1
D0 N0 H4RM: A Healthcare Security Conversation - FSL
Data Analysis for Detection Research Through Jupyter Notebooks 101 (Beginner) - BTWV2
DAY1 KEYNOTE: The Trust Talks - BHV
DAY2 KEYNOTE: Understanding DIYBio and Community Labs - A Social Science Approach - BHV
DAY3 KEYNOTE: Why is Security Hard? - BHV
Decentralization in a Centralized world - MOV
Decentralized Finance (DeFi) - ready for prime time ? - BCV
Deep Dive into Adversary Emulation - Ransomware Edition - RTV
DEF CON Groups Panel - DCG
Defending Your UNIX Hosts (Intermediate) - BTWV1
Demystifying Modern Windows Rootkits - DC
Deploying Pi-hole: More Than an Ad Blocker (Beginner) - BTWV1
Detecting Fake 4G Base Stations in Real Time - DC
Detecting hand-crafted social engineering emails with a bleeding-edge neural language model - AIV
Detecting The Not-PowerShell Gang (Intermediate) - BTVT1
Differential Privacy..more important than ever in the world of Covid-19 - CPV
Digital Health Technologies in the NIH All of Us Research Program - BHV
Discovering Cloud File Storage Artifacts - CLV
Discovering ELK The First Time - Lessons Learned Over 2 Years (Beginner) - BTVT1
Discovering Hidden Properties to Attack Node.js ecosystem - DC
Discussion: What makes a good ham radio operator? - HRV
Dissecting Wireless Privacy In Aviation - AEV
DIY Diabetics and a Million Boluses - BHV
Dj St3rling - ENT
DNS New World Order, version 1.4: QuadX! DoH! DoT! Da Fuq? - DCG
DNS Privacy - CPV
DNSSECTION: A practical attack on DNSSEC Zone Walking - DC
Domain Fronting is Dead, Long Live Domain Fronting: Using TLS 1.3 to evade censors, bypass network defenses, and blend in with the noise - DC
Don't Be Silly - It's Only a Lightbulb - DC
Don't Ruck Us Again - The Exploit Returns - DC
Don't Go Postal Over Mail In Voting - VMV
Doors, Cameras, and Mantraps OH MY! - LPV
Dos, Donts and How-Tos of crypto building blocks using Java - CPV
Double Spending in BSV, is it Possible? - BCV
DragonOS - How I kept busy during COVID19 - WLV
Drinks with Recruiters - CRV

Dumpster Fires: 6 Things About IR I Learned by Being a Firefighter - PHVT
EFF Tech Trivia Pub Quiz - CNE
Election Security - POV
Electronic Ballot Return Standards & Guidelines - VMV
Emulating an Adversary with Imperfect Intelligence - RTV
Entrepreneurial Adventures: What It Takes to Start A Company - CRV
Enumerating Cloud File Storage Gems - RTV
ERPwnage - a red team approach to targeting SAP - RTV
European regulatory trends for Artificial Intelligence: same impact on US as GDPR? - CPV
Evil Genius: Why you shouldn't trust that keyboard - RTV
Evil Printer: How to Hack Windows Machines with Printing Protocol - DC
Executing Red Team Scenarios with Built-in Scenario Place - RTV
Experimental Aviation, Risks And Rewards - AEV
exploit insecure crypto wallet - BCV
Exploiting Key Space Vulnerabilities in the Physical World - DC
Exploiting Spacecraft - AEV
Exploring vulnerabilities in Smart Sex Toys, the exciting side of IoT research - IOT
Faults in our Pi Stars: Security Issues and Challenges in Deep Reinforcement Learning - AIV
Fear and Loathing in Payment Bug Bounty - PAYV
Fear, Uncertainty, and Doubt about Human Microchip Implants - CPV
Federal Communications Commission - ETV
Federal Trade Commision - ETV
Fighting a Virus with a Spreadsheet (Beginner) - BTVT1
File Encryption For Actual Humans - CPV
Film Festival: Project Immerse: A Deepfake Paranoid Thriller - CNE
Film Festival: Project Immerse: A Deepfake Paranoid Thriller - CNE
Finding and Exploiting Bugs in Multiplayer Game Engines - DC
Fireside Chat with Dr. Amy Abernethy and Adama Ibrahim - BHV
Fireside Chat: All about Section 230, the EARN IT Act, and What They Mean for Free Speech and Encryption - CPV
Food and Drug Administration - ETV
From Barista to Cyber Security Pro, Breaking the Entry Level Barrier - CRV
From Blackbox to Automotive Ransomware - CHV
From Discovery to Disclosure - RTV
From Printers to Silver Tickets or Something (Rebroadcast) - PWDV
From Printers to Silver Tickets or Something - PWDV
Fundamentals of Diagnostic Requests over CAN Bus - CHV
Fundamentals of Diagnostic Requests over CAN Bus - CHV
Future Proofing Your Career - CRV
General Aviation (GA) Electronic Flight Bags (EFB) - AEV
Getting Advanced with Hashcat (Rebroadcast) - PWDV
Getting Advanced with Hashcat - PWDV
Getting Shells on z/OS with Surrogat Chains - DC
Getting Started – Building an IoT Hardware Hacking Lab - IOT
Getting Started with Hashcat (Rebroadcast) - PWDV
Getting Started with Hashcat - PWDV
Getting started with the Intervillage badge - MOV
Ghosting the PACS-man: New Tools and Techniques - WLW
Google Maps Hacks - RGV
Government Espionage on a School Lunch Budget - DCG
GPS Spoofing 101 - AEV
Graylog: An Introduction Into OpenSOC CTF Tools - BTVT1
Grey Hat SSH: SShenanigans - RTV
Guerrilla Red Team: Decentralize the Adversary - RTV
Hack the SeaPod - HTS
Hack the SeaPod - HTS

Hack-a-Fax - VMV
Hack-A-Sat Closing Segment - AEV
Hack-A-Sat End Of Day Recap - AEV
Hack-A-Sat Friday Recap - AEV
Hack-A-Sat Kickoff Segment - AEV
Hack-A-Sat Launch Party - AEV
Hacker Jeopardy - CNE
Hacker Jeopardy - CNE
HackerBox 0057 Build Session - HHV
HackerBox 0057 Build Session - HHV
Hackers And ISACS - AEV
Hacking Aerospace Cybersecurity Regulation - AEV
Hacking Airplane Air To Ground (A2G) Systems - AEV
Hacking Democracy II: On Securing an Election Under Times of Uncertainty and Upheaval - VMV
Hacking like Paris Hilton 14 years later - and still winning! - CPV
Hacking Ludicrous Mode on a Tesla (moar powerr!) - CHV
Hacking Security Leadership - CRV
Hacking smart-devices for fun and profit: From exploiting my smart-home into controlling thousands of smart-devices around the world - IOT
Hacking TESLA Model 3 - NFC Relay Revisited - CHV
Hacking the Hybrid Cloud - DC
Hacking the Insulin Supply Chain To Save Lives - BHV
Hacking the Supply Chain – The Ripple20 Vulnerabilities Haunt Hundreds of Millions of Critical Devices - DC
Hacking traffic lights - DC
Hacking with Skynet - How AI is Empowering Adversaries - AIV
Hacking Zoom: a Hacker's Journey into Zoom Security - RTV
Hackium: a browser for web hackers - ASV
Ham Radio USA License Exams (Friday) - HRV
Ham Radio USA License Exams (Saturday) - HRV
Ham Radio USA License Exams (Sunday) - HRV
Hardware hacking 101: There is plenty of room at the bottom - HHV
Hardware hacking 101: There is plenty of room at the bottom - HHV
Hashes; Smothered, Covered, and Scattered: Modern Password Cracking as a Methodology - RTV
Have my keys been pwned? - API Edition - RTV
Heightened Election Security Risks Admist the Pandemic - VMV
Hella Booters: Why IoT Botnets Aren't Going Anywhere - IOT
High Security Wafer Locks - An Oxymoron? - LPV
Houston, we CAV a problem - CHV
How Blue Penetrates You - CLV
How COVID19 Changed Our Understanding of Cyber Disaster Medicine - BHV
How I defeated the Western Electric 30c - LPV
How Independent Security Researchers work with Medical Device Manufacturers - The Bad, The Ugly & The Great (BUG) - BHV
How to get rights for hackers - IOT
How to Grow a Brain in a Jar - Neuroengineering 101 - BHV
How to hack SWIFT, SPID, and SPEI with basic hacking techniques (from a Red Team Perspective) - RTV
How to Start a Movement: Hackers Edition - ETV
How to store sensitive information in 2020? - CPV
How we recovered \$XXX,000 in Bitcoin from an encrypted zip file - DC
Hunting for Blue Mockingbird Coinminers - RCV
Hybrid PhySec tools - best of both worlds or just weird? - LPV
Hyperlocal Drift detection with Goko: Finding abusers of your Dataset - AIV
IAM Concerned: OAuth Token Hijacking in Google Cloud (GCP) - CLV
Icetre Normal - ENT
ICS Village CTF Kick-Off - ICS

Identifying and fixing out-of-gas errors in smart contracts with smart fuzzing - BCV
Identity Crisis: the mad rise of online account opening fraud - PAYV
ILS and TCAS Spoofing Demonstration - AEV
Importing vector graphics in to EagleCAD - HHV
In search of the perfect UPnP tool - IOT
In theory, there is no difference between theory and practice - CRV
Incident Response and the ATT&CK Matrix (Beginner) - BTWV2
Incident Response Panel - BTVT1
Indicators of Emulation (Intermediate) - BTVT1
Indicators of Emulation: Extra Spicy Adversary Emulation - RTV
Industrial Cybersecurity in Mexico - ICS
Infodemic: Threat models for patient communities on social networks - BHV
Initial Compromise through Web Side - RTV
Inside the Mind of a Threat Actor: Beyond Pentesting - RTV
Intro to DC603 - DCG
Intro to DC858 - DCG
Intro to high security locks and lockpicking - LPV
Intro to Lockpicking - LPV
Introducing DropEngine: A Malleable Payload Creation Framework - RTV
Introducing Melbourne DCG by Allen and Friends - DCG
Introducing the Meet a Mentor Program - BTVT1
Introduction To ACARS - AEV
Introduction to Malware Analysis & Response (MA&R) (Beginner) - BTWV1
Introduction to U-Boot Interaction and Hacking - IOT
Introduction to WiFi Security - WLW
Intrusion Analysis and Threat Hunting with Open Source Tools - PHVW
IoT Hacking Stories in Real Life - IOT
IoT Honey pots and taming Rogue appliances - IOT
IoT Under the Microscope: Vulnerability Trends in the Supply Chain - IOT
jeopardize - DL
jeopardize - DL
John Odum, Montpelier, VT - VMV
Journal Club Live! Fawkes FR - AIV
JWT Parkour - ASV
Key Duplication - It's not just for the movies! - LPV
Key Ingredients for the Job Interviews (Virtual or Face-2-Face) - CRV
Key Note - State of Blockchain Security - BCV
Keynote Remarks: Representative Jackie Speier - VMV
Keynote Remarks: Senator Ron Wyden - VMV
Keynote: Monero: Sound Money Safe Mode - MOV
Keynote: Monero: Sound Money Safe Mode - MOV
Keynote: Monero: Sound Money Safe Mode - MOV
Keynote - ICS
Keystone to the Kingdom - LPV

Kibana: An Introduction Into OpenSOC CTF Tools - BTVW1
Kicking Devices and Taking CVEs : The Zoomer's Guide to Hacking Shit - IOT
Killer Robots Reconsidered - ETV
Knock knock, who's there? Identifying assets in the cloud - RTV
Kubernetes Container Orchestration Security Assessment - ASV
Kubernetes Goat - Vulnerable by Design Kubernetes Cluster Environment - RTV
LadderLeak: Breaking ECDSA With Less Than One Bit Of Nonce Leakage - CPV
Lateral Movement and Privilege Escalation in GCP; Compromise any Organization Without Dropping an Implant - DC
Law School for Lockpickers - LPV
Learn to Solder the BadgeBuddy Kit - HHV
Learning to Use Logic Analyzers - IOT
Least privilege using infrastructure as code - CLV
Length 15 & No Change. Implementing NIST SP800-63B for real (Rebroadcast - PWDV
Leveraging the critical YARA skills for Blue Teamers (Beginner) - BTVW1
Live Q&A with Special Guests Regarding "Kill Chain" - VMV
Live SE Q&A - SEV
localghost: Escaping the Browser Sandbox Without 0-Days - ASV
Locha Mesh: Monero off-the-grid - MOV
Low Value Indicators For High Value Decisions (Intermediate) - BTVT1
Low-Cost VHF Receiver: Eavesdropping Pilot/Controller Communication - AEV
Making Breach and Attack Simulation Accessible and Actionable with Infection Monkey - from IT to the C-suite - RTV
Making Next Generation Drugs at Home - BHV
Making sense of EMV card data – decoding the TLV format - PAYV
Making Targeted Wordlists (Rebroadcast) - PWDV
Making Targeted Wordlists - PWDV
MalConfScan with Cuckoo - DL
Mechanizing the Methodology: Automating Discovery, Testing, and Alerting using Recon/Testing Tools and Amazon SES - RTV
Media Analysis of Disinformation Campaigns - PHVT
Medical Device Vulnerability Disclosure - BHV
Medical Technology: How do we unfuck things - BHV
MedICS - BHV
Meetup: 3H: Hardware Happy Hour - HHV
Meetup: Certification Processes (UL, FCC, etc.) - HHV
Meetup: Legacy Hardware - HHV
Meetup: OSS ASIC - HHV
Meetup: PCB Proto and Rework - HHV
Meetup: Some HHV Challenges - HHV
Meetup: Some HHV Challenges - HHV
Meetup: Some HHV Challenges - HHV
Meetup: Sourcing Parts - HHV
Meetup: Sourcing Parts - HHV
Meetup: Wearables - HHV
Mica Husky - ENT
Mis/Dis Information & Democracy - POV
Misbehavior Detection for V2X communication - CHV
Misinformation & Covid - AIV
Miss Jackalope - ENT
Mission Kill: Process Targeting in ICS Attacks - ICS
MITM - The Mystery In The Middle. An Introduction To The Aircraft Information Systems Domain - AEV
MITRE ICS ATT&CK - ICS

ML Security Evasion Competition 2020 - AIV
Mobile Security Framework - MobSF - DL
Modeling systematic threat: testing on mainnet fork - BCV
Models of Privacy Norms - ETV
Modern Red Team Tradecraft - Informing Defenders by Evolving Your Attackers - RTV
Monero Wallet Basics: Sending, Receiving, Proving - MOV
Monetary Maximalism and Millennial Finance - Building Decentralized Tooling to Empower Everyone - BCV
Movie Stream - Lost World - DC
NAND Flash – Recovering File Systems from Extracted Data - IOT
National Service Panel: Career Opportunities Supporting the Country - CRV
Next level stalker ware - CPV
Ninjula - ENT
No Question: Teamviewer, Police and Consequence (Beginner) - BTVT1
No Tech Talks - CNE
O365Squatting (Intermediate) - BTVT1
OBD and what we CAN do with it - CHV
OBD and what we CAN do with it - CHV
Offensive Embedded Exploitation : Getting hands dirty with IOT/Embedded Device Security Testing - RTV
Office Drama on macOS - DC
On the insecure nature of turbine control systems in power generation - ICS
onkeypress=hack(); - HHV
onkeypress=hack(); - HHV
Online Ads as a Recon and Surveillance Tool - CPV
Online Banking Security - PAYV
Online Voting: Theory and Practice - CPV
Only takes a Spark - Popping a shell on a 1000 nodes - DC
Open Live Chat for all Speakers or another talk on Ethics of Moderation - ETV
Open Office Q&A w/ Monero Research Lab's Sarang - MOV
Open Ventilator Remote Monitoring Project - BHV
Open-Source Tools for Hunting and Practical Intelligence (Intermediate) - BTVW1
Opening Remarks: Getting The Aerospace Village To Take-Off - AEV
Opening Remarks - AIV
Operationalizing Cyber Norms: Critical Infrastructure Protection - ICS
Osquery: An Introduction Into OpenSOC CTF Tools - BTVW1
OSTWERK Initiative - HRV
OU having a laugh? - RTV
Our journey into turning offsec mindset to developer's toolset - ASV
OuterHaven - The UEFI Memory Space Just Itching to be Misused (Intermediate) - BTVT1
Ours, Forces, and Equivoque: A treatise on how Magicians speak - RGV
OWASP API Top 10 - DCG
Packet Acquisition: Building the Haystack - PHVT
Pandemic In Plaintext - IOT
Panel: The Joy of Coordinating Vulnerability Disclosure - RTV
Password cracking beyond 15 characters and under \$500 - RTV
PathWell: Dynamic Password Strength Enforcement (Rebroadcast) - PWDV
PathWell: Dynamic Password Strength Enforcement - PWDV
PatrOwl - Red flavour of SOC automation - RTV
Peeling Back the Layers and Peering Through the Clouds with Security Onion - CLV
Performance - RGV
Performance - RGV
Phirautee - DL
Pickpocketing @ Home - RGV
Playing with Electricity: Hacking into Distribution Companies - ICS
Porcupine: Rapid and robust tagging of physical objects using DNA with highly separable nanopore signatures - BHV
PoS Terminal Security Uncovered - PAYV

PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS - ICS
PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS - CHV
Practical Advice on Threat Hunting Panel - BTVT1
Practical PCFG Password Cracking (Rebroadcast) - PWDV
Practical PCFG Password Cracking - PWDV
Practical VoIP/UC Hacking Using Mr.SIP: SIP-Based Audit & Attack Tool - DC
Practice 'Net' via Discord - HRV
Product Cybersecurity: Secure Airplane Development Lifecycle - AEV
Proposed Mitigation Measures to Address a Disruption Such as The Economic Impact of COVID -19 on Transaction Capacity and Fees in Monero - MOV
Protecting Elections with Data Science -- A Tool for 2020 and Beyond - VMV
Purple On My Mind: Cost Effective Automated Adversary Simulation (Intermediate) - BTVT1
PWN The World - RTV
Pwn2Own Qualcomm compute DSP for fun and profit - DC
Pwning Your Resume - CRV
PyRDP: Remote Desktop Protocol Monster-in-the-Middle (MITM) and Library - DL
PyRDP: Remote Desktop Protocol Monster-in-the-Middle (MITM) and Library - DL
Quantum Computers & Cryptography - CPV
Quark Engine - An Obfuscation-Neglect Android Malware Scoring System (Beginner) - BTVT1
Ransom in the Cloud - CLV
Realistic Trends in Vulnerability based on Hacking into Vehicle - CHV
Red Team Village Announcements and Remarks - RTV
Red Team Village Closing Ceremony and Announcement of Winners of CTF and CyberWraith - RTV
Red Team Village CTF - Finals - RTV
Red Team Village CTF - Prequal - RTV
Red Team Village Opening Remarks - RTV
Red Teaming: Born from the Hacker Community - RTV
Redefining patient safety in the digital era - BHV
redlure - DL
redlure - DL
RedTeamOps - Managing Red Team Infrastructure as a Red Teamer - RTV
Remediation Framework - Auto respond to AWS nightmares. - CLV
Remote Online Balloting Delivery and Marking Options and Security Considerations for Absentee Voting During the COVID-19 Pandemic - VMV
Result of Longer Passwords in Real World Application (Rebroadcast) - PWDV
Result of Longer Passwords in Real World Application - PWDV
Reverse Engineering the Tesla Battery Management System for Moar Powerrr! - DC
Reversing with Dynamic Data Resolver (DDR) – Best practice (Advanced) - BTVT1
Reviewing MS08-067, Illustration Of An Old Chapter - RTV
Rights You Can't Exercise Can't Protect You: Privacy by Design, Dark Patterns, and Cultural Context - CPV
Rogues adventure & the intervillage badge - RGV
Rogues Village Introduction - RGV
Room for Escape: Scribbling Outside the Lines of Template Security - DC
Running an appsec program with open source projects - ASV
Russian Cyber Threats in The Pandemic Era - BHV
SaaSocalypse - The Complexity and Power of AWS Cross Account Access - CLV
Safecracking for Everyone! - LPV
Satellite Orbits 101 - AEV
Saving Yourself from Microsoft: It's by design - DCG
Secretary Kim Wyman, Washington - VMV
Secure Your Code — Injections and Logging - ASV
Securing AND Pentesting the Great Spaghetti Monster (k8s) - RTV
Securing the COSMOS: How to operate and secure a validator - BCV
Security Focused Operating System Design - BCV
Security of Election Systems: A contract case study in progress - ETV

See Something, Say Something - VMV
Shadowvex - ENT
Shrek, Juggs, and Toxic Trolls: a BADASS discussion about Online Sexuality and Hacktivism - FSL
Single Board Computers in Amateur Radio - HRV
Skittish & Bus - ENT
So You Got an SDR: Common Signals and the Wiki - HRV
Sounds Legit: Why you shouldn't trust that speaker - RTV
Spectra—New Wireless Escalation Targets - DC
Spectrum: An End-to-End Framework for ML-based Threat Monitoring and Detection - AIV
Speed 2: The Poseidon Adventure – When Cruise Ships Go Wrong - HTS
Starkiller - DL
Starkiller - DL
STARTTLS is Dangerous - CPV
Static analysis of Infrastructure as code: Terraform, Kubernetes, Cloudformation and more! - CLV
Stepped on a Nail - IOT
Subxian - ENT
Suricata: An Introduction Into OpenSOC CTF Tools - BTWV1
Take Down the Internet! With Scapy - PHVT
Talking to Satellites - HRV
Talking To Satellites - 101 - AEV
TechCongress - ETV
tense future - ENT
Terrestrial Access Network - ENT
The Art of Balancing: A Burnout Talk - RTV
The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections - VMV
The Basics Of Breaking BLE v3 - WLV
The Bug Hunter's Methodology - RTV
The DevOps & Agile Security Toolkit - ASV
The Elephant in the Room: Burnout - ASV
The future of IoT Security “Baselines, Standards, and Regulatory Domain - IOT
The Individual Contributor to Tech Executive, or There and Back Again - CRV
The Journey of ICS Project Files - Visibility and Forensics to Exploitation - ICS
The Joy of Coordinating Vulnerability Disclosure - IOT
The K0BAK Rover Van - HRV
The Norwegian Blue: A lesson in Privacy Engineering - CPV
The Student Roadmap to Becoming A Penetration Tester - RTV
The Underestimated Threat Vector: Homogeneity - BHV
The Vulnerability That Gmail Overlooked and Enabling Threat Hunting - PHVT
The Worst Mobile Apps - PHVT
This year's village badge - MOV
Threagile - Agile Threat Modeling with Open-Source Tools from within Your IDE - ASV
Threat Hunting with the Elastic Stack (Beginner) - BTWV2
Threat Modelling the Death Star - ASV
Ticketing To Takeoff: An Airport Hacking Choose Your Own Adventure - AEV
Total E(A)gression - RTV
Towards an Institutional Review Board for Biohackers - BHV
Tracer FIRE 9 (Intermediate) - BTWV1
Trends in the online card payment security - PAYV
Tricky Bundles: Smarter Dependency Management for I2P-Bundling Applications - MOV
Trust And Truth In Space Situational Awareness - AEV
Trust, but Verify: Maintaining Democracy In Spite of - RTV
Turning Telemetry and Artifacts Into Information (Intermediate) - BTWV1
Twitter Word Phrequency - RCV
Twitter's Tax Day Disaster: The Beginning (and End) of Mainstream Crypto Scams - BCV

U.S. Privacy and Civil Liberties Oversight Board Member - ETV
Understanding Cyber-Attacks and Their Implications to Democratic Regimes - VMV
Understanding the Threat: Malicious Software, Malicious Actors, and the Promise of Connected Medical Technology - DCG
Velociraptor: An Introduction Into OpenSOC CTF Tools - BTWV1
Verifiable Delay Functions for preventing DDoS Attacks on Ethereum 2.0 - BCV
Veteran Transition Tips - CRV
Village Closing Commentary - HRV
Village Opening Remarks - HRV
Violent Python 3 - PHVW
Vivisection PowerPC - ICS
Vote @ Home Workshop - ETV
Vote-from-home? Review of Election Security on Remote Voting in Response to COVID-19 - VMV
Vulnerability Discovery - Tips for Surviving and Thriving - ICS
War By Other Means: How Influence Operations Undermine Democracy - VMV
War Story Bunker - CNE
Weaponized XSS - Moving Beyond Alert(1) - RTV
Web Shell Hunting - Part 1 - ASV
Web Shell Hunting - Part 2 - ASV
Welcome and Kick-Off - VMV
Welcome Speech - MOV
Welcome to DEF CON Safe Mode - DC
Welcome to the Payment Village - PAYV
What college kids always get wrong, the art of attacking newbies to blueteam - RTV
What I Learned Trying To Hack A 737 - AEV
What if we had TLS for phone numbers? An introduction to SHAKEN/STIR - CPV
What the Shuck? Layered Hash Shucking (Rebroadcast) - PWDV
What the Shuck? Layered Hash Shucking - PWDV
What's up with proposed privacy legislation and how to influence the debate - BHV
When TLS Hacks You - DC
Whispers Among the Stars: Perpetrating (and Preventing) Satellite Eavesdropping Attacks - DC
Who needs spyware when you have COVID-19 apps? A look at global trends and what to do about it. - CPV
Who's secure, who's not, & who makes that choice - ASV
Whose Slide is It Anyway - CNE
wicked wardriving with gps and glonass - WLV
Wireless Blue Team - WLV
Wireless Village Fireside Talk - WLV
Wireshark for Incident Response & Threat Hunting (Beginner) - BTWV2
Wireshark for Incident Response & Threat Hunting - PHVW
Workshop: Let's Talk About Abusability Testing - CPV
Workshop: Let's Talk About Abusability Testing - CPV
Workshop: Let's Talk About Abusability Testing - CPV
Writing Wireshark Plugins for Security Analysis - PHVW
Y'all Tryna Bypass Python 3.8 Audit Hooks or Nah? - RTV
Yacht PWNed - HTS
Yippee-Ki-Yay MFA'er - Bypassing Multi-Factor Authentication with Real-Time Replay Session Instantiation Attacks - RTV
You're Adversary Within - The Golden Age of Insider Threats - RTV
You're not the money printer, or why we need to separate coinbase rings - MOV
Your connected world isn't yours anymore! - Remote IoT attacks and data exfiltration. - IOT
Zebbler Encanti Experience - ENT
Zeek: An Introduction Into OpenSOC CTF Tools - BTWV1
Zero Trust - A Vision for Securing Cloud and Redefining Security - RTV

Village Talk List

AeroSpace Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#av-lounge-bar-text](#)

PDT Times	Title	speaker
Friday		
08:00 - 08:25	Hack-A-Sat Launch Party	
08:30 - 15:59	Hack-a-Sat	
08:00 - 19:59	A-ISAC CTF	
09:00 - 15:59	Cal Poly Workshop - Simulated Satellite Communicat . . .	
09:00 - 15:59	Deep Space Networking	
09:00 - 15:59	Nyan Sat Workshop	
09:00 - 15:59	Aviation Privacy Treasure Hunt	Martin Strohmeier
09:00 - 15:59	Mission Alenium: Launching the Next Generation int . . .	Henry Danielson
10:00 - 10:59	Opening Remarks: Getting The Aerospace Village To . . .	Chris Krebs,Dr Will Roper . . .
10:00 - 13:30	Understanding Space Through a CyberSecurity Lens	
11:00 - 11:59	MITM - The Mystery In The Middle. An Introduction . . .	Matt Gaffney
12:00 - 12:30	Satellite Orbits 101	Matt Murray
12:30 - 12:59	GPS Spoofing 101	Harshad Sathaye
12:00 - 17:59	Bricks in the Air	
12:00 - 17:59	CPX SimpleSat	
12:00 - 17:59	DDSAT-1	
13:00 - 13:59	Building Connections Across The Aviation Ecosystem	Katie Noble,Al Burke,Jeff . . .
14:00 - 14:59	Experimental Aviation, Risks And Rewards	Patrick Kiley
14:30 - 17:59	Understanding Space Through a CyberSecurity Lens	
15:00 - 15:59	Talking To Satellites - 101	Eric Escobar
16:00 - 16:30	Hack-A-Sat Friday Recap	
17:00 - 17:59	Exploiting Spacecraft	Brandon Bailey
Saturday		
08:30 - 08:59	Attacking Flight Management Systems: This Is Your . . .	Javad Dadgar,Mohammad-Rez . . .
08:00 - 19:59	A-ISAC CTF	
09:00 - 09:30	Hack-A-Sat Kickoff Segment	
09:30 - 09:59	Aerospace Village Badge	Rick Hansen
09:30 - 15:59	Hack-a-Sat	
09:00 - 15:59	Bricks in the Air	
09:00 - 15:59	Cal Poly Workshop - Simulated Satellite Communicat . . .	
09:00 - 15:59	CPX SimpleSat	
09:00 - 15:59	DDSAT-1	
09:00 - 15:59	Deep Space Networking	
09:00 - 15:59	Nyan Sat Workshop	

PDT Times	Title	speaker
09:00 - 12:30	Understanding Space Through a CyberSecurity Lens	
09:00 - 15:59	Mission Alenium: Launching the Next Generation int . . .	Henry Danielson
10:00 - 10:59	Hackers And ISACS	Erin Miller,Jeff Troy,Ken . . .
11:00 - 11:30	A View From The Cockpit: Exploring Pilot Reactions . . .	Matt Smith
11:30 - 11:59	Checklist For Aviation Vulnerability Disclosure: D . . .	Jay Angus
12:00 - 12:59	Low-Cost VHF Receiver: Eavesdropping Pilot/Control . . .	Allan Tart,Fabian Landis
13:00 - 13:30	Product Cybersecurity: Secure Airplane Development . . .	Michael Vanguardia
13:30 - 13:59	Introduction To ACARS	Alex Lomas
13:30 - 16:59	Understanding Space Through a CyberSecurity Lens	
14:00 - 14:59	Ticketing To Takeoff: An Airport Hacking Choose Yo . . .	Liz Wharton
15:00 - 15:30	ILS and TCAS Spoofing Demonstration	Alex Lomas
15:30 - 15:59	A Deeper Dive Into ILS And ADS-B Spoofing	Harshad Sathaye
16:00 - 16:30	Hack-A-Sat End Of Day Recap	
17:00 - 17:59	General Aviation (GA) Electronic Flight Bags (EFB)	David Robinson
Sunday		
08:30 - 08:59	Hacking Airplane Air To Ground (A2G) Systems	Ali Abdollahi
09:00 - 09:59	Hacking Aerospace Cybersecurity Regulation	Harley Geiger,Kaylin Tryc . . .
09:00 - 13:59	Hack-a-Sat	
09:00 - 13:59	Bricks in the Air	
09:00 - 15:59	Cal Poly Workshop - Simulated Satellite Communicat . . .	
09:00 - 13:59	CPX SimpleSat	
09:00 - 13:59	DDSAT-1	
09:00 - 15:59	Deep Space Networking	
09:00 - 13:59	Nyan Sat Workshop	
09:00 - 12:30	Understanding Space Through a CyberSecurity Lens	
10:00 - 10:30	Trust And Truth In Space Situational Awareness	James Pavur
10:30 - 10:59	747 Walkthrough From A Hacker's Perspective	Alex Lomas,Ken Munro
11:00 - 11:59	Critical Aerospace Cybersecurity: How Hacking And . . .	Lawrence Rowell,Nathalie . . .
12:00 - 12:59	Cybersecurity Lessons Learned From Human Spaceflig . . .	Pam Melroy
13:00 - 13:30	Dissecting Wireless Privacy In Aviation	Martin Strohmeier
13:30 - 13:59	Breakdown Of The FAA's Privacy ICAO Address Progra . . .	Gui Michel
14:00 - 14:59	Hack-A-Sat Closing Segment	
15:00 - 15:59	Cybersecurity Meets Aviation Regulation	Aaron Cornelius,Tim Brom
16:00 - 16:59	What I Learned Trying To Hack A 737	Karl Koscher

[Return to Index](#)

Artificial Intelligence Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#aiv-general-text](#)

PDT Times	Title	speaker
Friday		
09:30 - 09:59	Opening Remarks	AI Village Organizers
10:00 - 10:30	ML Security Evasion Competition 2020	drhyrum,zh4ck
10:30 - 10:59	Baby's First 100 MLSec Words	erickgalinkin
11:00 - 12:30	Workshop 1	
13:00 - 13:30	Hyperlocal Drift detection with Goko: Finding abus . . .	comathematician
13:30 - 13:59	Spectrum: An End-to-End Framework for ML-based Thr . . .	Nahid Farhady
14:00 - 14:50	Hacking with Skynet - How AI is Empowering Adversa . . .	GTKlondike
15:00 - 15:59	Breakout Session	
16:00 - 17:30	Workshop 2	
Saturday		
09:30 - 09:59	"SECRETS ARE LIES, SHARING IS CARING, PRIVACY IS T . . .	Nahid Farhady
10:00 - 10:30	Misinformation & Covid	Imeyerov
11:00 - 12:30	Workshop 3	
13:00 - 13:59	Journal Club Live! Fawkes FR	AI Village Journal Club
14:00 - 14:59	Does AI Live up to the Hype?	
15:00 - 15:30	AI vs. Airplanes and IT-Security: What Security Re . . .	Laurin Weissinger
16:00 - 17:30	Workshop 4	
Sunday		
09:00 - 09:30	Detecting hand-crafted social engineering emails w . . .	Younghoo Lee,Joshua Saxe
10:00 - 10:59	Journal Club Live! Summoning Demons: The Pursuit o . . .	
13:00 - 13:59	Faults in our Pi Stars: Security Issues and Challe . . .	Vahid Behzadan
14:00 - 14:59	Ethics & Bias Panel	
15:30 - 15:59	Closing Remarks	

[Return to Index](#)

Applications Security Village

Friday: 09:00-18:00, Saturday: 09:00-17:00, Sunday: 09:00-15:00

Location: [#asv-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Who's secure, who's not, & who makes that choi . . .	Maddie Stone
11:00 - 11:45	2FA in 2020 and Beyond	Kelley Robinson
11:00 - 12:59	Applying Pysa to Identify Python Security Vulnerab . . .	Graham Bleaney
12:00 - 12:45	Android Bug Foraging	João Morais,Pedro Umbeli . . .
13:00 - 13:45	Our journey into turning offsec mindset to develop . . .	Paul Amar,Stanislas Molve . . .
15:00 - 15:45	API (in)Security TOP 10: Guided tour to the Wild W . . .	David Sopas,Paulo Silva
16:00 - 16:45	Threat Modelling the Death Star	Mário Areias
16:00 - 17:59	JWT Parkour	Louis Nyffenegger
Saturday		
09:00 - 09:59	Be Like Water: What Bruce Lee Can Teach Us About A . . .	Fredrick "Flee" Lee
10:00 - 10:59	Web Shell Hunting - Part 1	Joe Schottman
10:00 - 10:45	10,000 Dependencies Under The Sea: Exploring and S . . .	Gregg Horton,Ryan Slama
11:00 - 11:45	Hackium: a browser for web hackers	Jarrold Overson
12:00 - 12:45	The DevOps & Agile Security Toolkit	David Waldrop
12:00 - 13:59	Web Shell Hunting - Part 2	Joe Schottman
13:00 - 13:45	localhost: Escaping the Browser Sandbox Without 0 . . .	Parsia Hakimian
15:00 - 15:45	Can't Touch This: Detecting Lateral Movement in Ze . . .	Phillip Marlow
Sunday		
09:00 - 09:45	Threagile - Agile Threat Modeling with Open-Source . . .	Christian Schneider
10:00 - 11:59	Kubernetes Container Orchestration Security Assess . . .	Ali Abdollahi
10:00 - 10:45	The Elephant in the Room: Burnout	Chloé Messdaghi
11:00 - 11:45	A Heaven for Hackers: Breaking a Web Security Virt . . .	Mehmet D. Ince
12:00 - 12:45	Secure Your Code — Injections and Logging	Philipp Krenn
13:00 - 13:45	Running an appsec program with open source project . . .	Vandana Verma Sehgal

[Return to Index](#)

Block Chain Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#bcv-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:10	Welcome Note	
10:10 - 10:59	Key Note - State of Blockchain Security	Peter Kacherginsky
11:00 - 11:59	Verifiable Delay Functions for preventing DDoS Att . . .	Gokul Alex,Tejaswa Rastog . . .
12:00 - 12:59	Security Focused Operating System Design	Colin Cantrell
13:00 - 13:30	Cryptocurrencies have superusers?	Mark Nesbitt
13:30 - 13:59	Double Spending in BSV, is it Possible?	Poming Lee
14:00 - 14:59	Creating a decentralized storage for Kubernetes wi . . .	Kevin Leffew
15:00 - 15:59	Attacking and Defending Blockchain Nodes	Peter Kacherginsky
16:00 - 16:59	Panel Discussion	
Saturday		
10:00 - 10:10	Welcome Note	
10:10 - 10:59	Twitter's Tax Day Disaster: The Beginning (and E . . .	Victor Fang
11:00 - 11:59	Decentralized Finance (DeFi) - ready for prime ti . . .	Ryan Rubin
12:00 - 12:59	Securing the COSMOS: How to operate and secure a v . . .	Ron Stoner
13:00 - 13:30	Blockchain for Cyber Defense: Will it be as good a . . .	Seungjoo,Suhyeon Lee
13:30 - 13:59	Identifying and fixing out-of-gas errors in smart . . .	Sebastian Banescu
14:00 - 14:59	Monetary Maximalism and Millennial Finance - Build . . .	Kris Jones,Matt Luongo
15:00 - 15:59	7 Phases of Smart Contract Hacking	Martin Abbatemarco
16:00 - 16:59	Panel Discussion	
Sunday		
10:00 - 10:10	Welcome Note	
10:10 - 10:59	Modeling systematic threat: testing on mainnet for . . .	Martinet Lee
11:00 - 11:59	Building a Microcontroller Bitcoin Address Generat . . .	chaintuts,Josh McIntyre
12:00 - 12:40	exploit insecure crypto wallet	Minzhi He,peiyu wang
12:40 - 12:59	Closing Note	

[Return to Index](#)

Bio Hacking Village

Thursday: 0900 - 18:00, Friday: 10:00 - 18:00 , Saturday: 10:00 - 18:00 , Sunday: 10:00 - 15:00 (CTF closes at 1200 PT)

Location: [#bhv-general-text](#)

PDT Times	Title	speaker
Friday		
09:30 - 10:45	DAY1 KEYNOTE: The Trust Talks	Nina Alli, Vee Schmitt, Yus . . .
11:00 - 11:45	Fireside Chat with Dr. Amy Abernethy and Adama Ibr . . .	Adama Ibrahim, Amy Abernet . . .
11:30 - 11:59	Porcupine: Rapid and robust tagging of physical ob . . .	Katie Doroschak
12:00 - 12:59	Redefining patient safety in the digital era	Dena Medelsohn, Jen Goldsa . . .
13:00 - 13:59	Russian Cyber Threats in The Pandemic Era	Dr. Khatuna Mshvidobadze
14:00 - 14:30	Digital Health Technologies in the NIH All of Us R . . .	Michelle Holko
14:30 - 15:30	Medical Device Vulnerability Disclosure	Chloé Messdaghi, Eirick L . . .
15:30 - 15:59	Hacking the Insulin Supply Chain To Save Lives	Anthony DiFranco
16:15 - 16:45	Cybersecurity informed consent for medical devices	
16:45 - 17:45	INCLUDES NO DIRT: Threat Modeling for Healthcare	
Saturday		
10:00 - 10:45	DAY2 KEYNOTE: Understanding DIYBio and Community L . . .	Yong-Bee
11:00 - 11:30	How COVID19 Changed Our Understanding of Cyber Dis . . .	Christian “quaddi Da . . .
12:00 - 12:30	Medical Technology: How do we unfuck things	Veronica
12:30 - 13:30	Advancing Medical Device Security – How collabor . . .	Mitchell Parker
14:00 - 14:30	MedICS	Bryson Bort
14:45 - 15:15	Towards an Institutional Review Board for Biohacke . . .	Dr. Sarah Blossom Ware
15:15 - 15:59	DIY Diabetics and a Million Boluses	Dr. Mike Rushanan, Julian . . .
16:00 - 16:30	Chinese Military Labratory Mission + COVID-19	The Red Dragon
16:30 - 17:30	What's up with proposed privacy legislation and ho . . .	Lucia Savage
Sunday		
10:00 - 10:59	DAY3 KEYNOTE: Why is Security Hard?	Seth Carmody
10:30 - 10:59	Infodemic: Threat models for patient communities o . . .	Andrea Downing
11:00 - 11:59	How Independent Security Researchers work with Med . . .	Kyle Erickson, Natali, Pete . . .
12:30 - 12:59	How to Grow a Brain in a Jar - Neuroengineering 10 . . .	Jack
13:15 - 13:45	The Underestimated Threat Vector: Homogeneity	Vidya Murthy
13:30 - 14:30	Making Next Generation Drugs at Home	Mixæl Swan Laufer
14:00 - 14:30	Open Ventilator Remote Monitoring Project	
14:45 - 16:45	Securing Your Medical Device Network on a Shoestri . . .	

[Return to Index](#)

Blue Team Village Talks 1

Friday: 09:00 - 18:00, Saturday: 09:00 - 18:00, Sunday: 09:00 - 18:00

Location: [#btv-general-text](#)

PDT Times	Title	speaker
Thursday		
09:00 - 09:59	Blue Team Village - Opening Ceremony	
10:15 - 10:59	Graylog: An Introduction Into OpenSOC CTF Tools	Lennart Koopmann
Friday		
10:00 - 10:30	Quark Engine - An Obfuscation-Neglect Android Malw ...	JunWei Song,KunYu Chen
11:00 - 11:59	OuterHaven - The UEFI Memory Space Just Itching to ...	Connor Morley
12:30 - 12:59	No Question: Teamviewer, Police and Consequence (B ...	corvusactual
13:30 - 14:30	Building BLUESPAWN: An Open-Source, Active Defense ...	Jake Smith,Jack McDowell
15:00 - 15:30	Indicators of Emulation (Intermediate)	Ch33r10
16:00 - 16:30	Detecting The Not-PowerShell Gang (Intermediate)	Mangatas Tondang
17:00 - 17:59	Discovering ELK The First Time - Lessons Learned O ...	TheDrPinky
18:30 - 18:59	Fighting a Virus with a Spreadsheet (Beginner)	Allen Baranov
19:30 - 20:30	Purple On My Mind: Cost Effective Automated Advers ...	Mauricio Velazco
Saturday		
09:00 - 09:59	Reversing with Dynamic Data Resolver (DDR) – Bes ...	Holger Unterbrink
10:30 - 10:59	O365Squatting (Intermediate)	Juan Francisco,Jose Migue ...
11:30 - 11:59	Low Value Indicators For High Value Decisions (Int ...	Allan Stojanovic,Spencer ...
12:30 - 13:30	Incident Response Panel	Russell Mosley,Vyrus,Litm ...
14:00 - 14:59	Blue Team Village & Red Team Village Panel	Joseph Mlodzianowski (c ...
15:30 - 16:30	Practical Advice on Threat Hunting Panel	Plug,Roberto Rodriguez,To ...
17:00 - 17:59	Introducing the Meet a Mentor Program	Scoubi,Plug,Litmoose,Xavi ...
Sunday		
16:00 - 16:59	Blue Team Village Closing Ceremony	

[Return to Index](#)

Blue Team Village Workshops 1

Friday: 09:00 - 18:00, Saturday: 09:00 - 18:00, Sunday: 09:00 - 18:00

Location: [#btv-general-text](#)

PDT Times	Title	speaker
Thursday		
11:15 - 11:59	Kibana: An Introduction Into OpenSOC CTF Tools	TimDotZero
12:15 - 12:59	OpenSOC CTF Tool Demo: Moloch	
13:15 - 13:59	Osquery: An Introduction Into OpenSOC CTF Tools	Whitney Champion
14:15 - 14:59	Velociraptor: An Introduction Into OpenSOC CTF Too . . .	Mike Cohen
15:15 - 15:59	Zeek: An Introduction Into OpenSOC CTF Tools	Aaron Soto,Amber Graner
16:15 - 16:59	Suricata: An Introduction Into OpenSOC CTF Tools	Josh
17:15 - 17:59	OpenSOC CTF Tool Demo: Thinkst Canary	
Friday		
10:00 - 11:30	Cypher for Defenders: Leveraging Bloodhound Data B . . .	Scoubi
13:30 - 14:59	Turning Telemetry and Artifacts Into Information (. . .	Omenscan
16:30 - 17:59	Open-Source Tools for Hunting and Practical Intell . . .	Joe Slowik
Saturday		
09:00 - 10:30	Leveraging the critical YARA skills for Blue Teame . . .	David Bernal Michelena
12:00 - 13:30	Tracer FIRE 9 (Intermediate)	Andrew Chu
15:30 - 16:15	Defending Your UNIX Hosts (Intermediate)	Daniel Ward,Samuel Gaspar . . .
Sunday		
09:00 - 10:30	Introduction to Malware Analysis & Response (MA&R) . . .	Michael Wylie
12:00 - 13:30	Deploying Pi-hole: More Than an Ad Blocker (Beginn . . .	Ben Hughes
15:00 - 15:45	Azure AD Logs for the Blue Team (Intermediate)	Mark Morowczynski

[Return to Index](#)

Blue Team Village Workshops 2

Friday: 09:00 - 18:00, Saturday: 09:00 - 18:00, Sunday: 09:00 - 18:00

Location: [#btv-general-text](#)

PDT Times	Title	speaker
Friday		
11:30 - 13:30	An Introduction to Hunting Adversaries Using the A...	Ben Bornholm
15:00 - 16:30	Threat Hunting with the Elastic Stack (Beginner)	Ben Hughes
18:00 - 19:30	Data Analysis for Detection Research Through Jupyt...	Roberto Rodriguez,Jose Ro...
Saturday		
10:30 - 11:59	Wireshark for Incident Response & Threat Hunting (...)	Michael Wylie
13:30 - 15:30	An Introduction to Hunting Adversaries Using the A...	Ben Bornholm
16:30 - 17:59	A N00b's Intro to Building Your Own Lab (Beginner)	Omar Santos
Sunday		
10:30 - 11:59	Incident Response and the ATT&CK Matrix (Beginner)	Sam Bowne
13:30 - 14:59	Cloud Security Monitoring on a Dime Store Budget (...)	Wes Lambert

[Return to Index](#)

Car Hacking Village

Friday: 10:00-17:00, Saturday: 10:00-17:00, Sunday: 10:00-12:00

Location: [#chv-welcome-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Adding new features by manipulating CAN bus	Teejay
10:00 - 10:50	Automotive In-Vehicle Networks	Kamel Ghali
11:00 - 11:59	PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS	Ben Gardiner,Chris Poore
11:00 - 11:50	OBD and what we CAN do with it	Infenet
12:00 - 12:59	Before J1939: A J1708/J1587 Protocol Decoder	Thomas Hayes,Dan Salloum
12:00 - 12:50	Fundamentals of Diagnostic Requests over CAN Bus	Robert Leale (CarFuCar)
13:00 - 13:50	Cluster fuzz!	Mintynet
14:00 - 14:59	Realistic Trends in Vulnerability based on Hacking . . .	Ryosuke Uematsu,Shogo Nak . . .
14:00 - 14:50	Bluetooth Security in Automotive	Kamel Ghali
15:00 - 15:59	CAN be super secure: Bit Smashing FTW	Brent Stone
15:00 - 15:50	Automotive Ethernet for the rest of us	Infenet
16:00 - 16:59	Misbehavior Detection for V2X communication	Jaime
16:00 - 16:50	Car (to Cloud) Talk: Using MQTT for Car Hacking	Jaime
Saturday		
10:00 - 10:59	Hacking TESLA Model 3 - NFC Relay Revisited	Huajiang "Kevin2600" Chen . . .
10:00 - 10:50	Automotive In-Vehicle Networks	Kamel Ghali
11:00 - 11:50	OBD and what we CAN do with it	Infenet
12:00 - 12:59	Houston, we CAV a problem	Vic Harkness
12:00 - 12:50	Fundamentals of Diagnostic Requests over CAN Bus	Robert Leale (CarFuCar)
13:00 - 13:59	CMAP: Open Source Vehicle Services Mapping Tool fo . . .	Robert Leale (CarFuCar)
13:00 - 13:50	Cluster fuzz!	Mintynet
14:00 - 14:59	All Aboard the CAN Bus... or Motorcycle	Derrick (CanBusDutch)
14:00 - 14:50	Bluetooth Security in Automotive	Kamel Ghali
15:00 - 15:59	From Blackbox to Automotive Ransomware	Nils Weiss,Enrico Pozzobo . . .
15:00 - 15:50	Automotive Ethernet for the rest of us	Infenet
16:00 - 16:59	ChupaCarBrah: Open Source Hardware and Software fo . . .	Marcelo Sacchetin
16:00 - 16:50	Car (to Cloud) Talk: Using MQTT for Car Hacking	Jaime
Sunday		
10:00 - 10:59	Hacking Ludicrous Mode on a Tesla (moar powerrr!)	Patrick Kiley

[Return to Index](#)

Cloud Village

Friday: 10:00-16:30, Saturday: 10:00-17:30, Sunday: 10:00-14:00

Location: [#cloudv-general-text](#)

PDT Times	Title	speaker
Friday		
06:00 - 12:30	Cloud Village CTF	
11:00 - 11:20	Opening Keynote	
11:20 - 12:05	IAM Concerned: OAuth Token Hijacking in Google Clo . . .	Jenko Hwong
12:05 - 12:50	Ransom in the Cloud	Spencer Gietzen
12:50 - 13:25	Static analysis of Infrastructure as code: Terrafo . . .	Barak Schoster
13:25 - 14:10	Can't Touch This: Detecting Lateral Movement in Ze . . .	Phillip Marlow
14:10 - 16:30	Peeling Back the Layers and Peering Through the Cl . . .	Wes Lambert
Saturday		
11:00 - 11:45	Least privilege using infrastructure as code	Nimrod Kor
11:45 - 12:30	How Blue Penetrates You	Dani Goland,Mohsan Farid
12:30 - 13:15	21 Jump Server: Going Bastionless in the Cloud	Colin Estep
13:15 - 13:59	Cloud Frontier	Setu Parimi
14:00 - 14:45	Attacking the Helmsman	Mohit Gupta
14:45 - 15:30	SaaSocalypse - The Complexity and Power of AWS Cr . . .	Alexandre Sieira
15:30 - 17:30	Discovering Cloud File Storage Artifacts	Michael Wylie
Sunday		
11:00 - 11:45	Cloud host base strategy by staging defensive tool . . .	Michael Mimo
11:45 - 12:30	Remediation Framework - Auto respond to AWS nightm . . .	Sahir Khan,Justin Paglier . . .
12:30 - 13:30	Cloud-Native Attack Detection and Simulation.	Nick Jones
13:30 - 13:50	Closing Note	

[Return to Index](#)

Contests and Events

Each Contest or Event has a Discord Channel. Check the [DC28 CNE](#) page for more info.

PDT Times	Title	speaker
Thursday		
09:00 - 17:59	Darknet Contest	
Friday		
06:00 - 15:59	SEATF: Maritime Hacking CTF	
09:00 - 17:59	AppSec Village CTF	
09:00 - 17:59	Be the Match - registration drive	
09:00 - 17:59	Bio-Hacking - Hospital Under Siege	
09:00 - 17:59	Capture The Packet (CTP)	
09:00 - 17:59	Car Hacking Village CTF	
09:00 - 17:59	CMD+CTRL CyberRange	
09:00 - 17:59	Crack Me If You Can (CMIYC)	
09:00 - 17:59	Darknet Contest	
09:00 - 17:59	(Before Con) Creative Writing Short Story Contest	
09:00 - 17:59	Coindroids	
09:00 - 17:59	The Gold Bug – Crypto and Privacy Village Puzzle	
09:00 - 17:59	Hackfortress	
09:00 - 17:59	H@cker Runw@y	
09:00 - 17:59	HomebrewHardware Contest	
09:00 - 17:59	ICS Hack the Plan[e]t	
09:00 - 17:59	Defcon Ham Radio Fox Hunting Contest	
09:00 - 17:59	Online MUD - EvilMog	
09:00 - 17:59	The Schemaverse Championship	
09:00 - 23:59	TeleChallenge	
09:00 - 23:59	ULTIMATE Secure Coding Throwdown (Secure Code Warr ...	
09:00 - 17:59	Wireless Capture the Flag	
09:00 - 17:59	Io57 Mystery Challenge	
09:00 - 17:59	OSINTSECCryptoAIBlockchain	
09:00 - 17:59	Social Engineer SECTF4Teens	
10:00 - 19:59	DEF CON Scavenger Hunt	
10:00 - 23:59	OpenSOC Blue Team CTF - General Round	
17:00 - 18:59	EFF Tech Trivia Pub Quiz	
18:00 - 19:59	War Story Bunker	
18:00 - 19:59	Hacker Jeopardy	
Saturday		
00:00 - 23:59	TeleChallenge	
00:00 - 23:59	ULTIMATE Secure Coding Throwdown (Secure Code Warr ...	
06:00 - 15:59	SEATF: Maritime Hacking CTF	

PDT Times	Title	speaker
09:00 - 17:59	AppSec Village CTF	
09:00 - 17:59	Be the Match - registration drive	
09:00 - 17:59	Bio-Hacking - Hospital Under Siege	
09:00 - 17:59	Capture The Packet (CTP)	
09:00 - 17:59	Car Hacking Village CTF	
09:00 - 17:59	CMD+CTRL CyberRange	
09:00 - 17:59	Crack Me If You Can (CMIYC)	
09:00 - 17:59	Darknet Contest	
09:00 - 17:59	(Before Con) Creative Writing Short Story Contest	
09:00 - 17:59	Coindroids	
09:00 - 17:59	The Gold Bug – Crypto and Privacy Village Puzzle	
09:00 - 17:59	Hackfortress	
09:00 - 17:59	H@cker Runw@y	
09:00 - 17:59	HomebrewHardware Contest	
09:00 - 17:59	ICS Hack the Plan[e]t	
09:00 - 17:59	Defcon Ham Radio Fox Hunting Contest	
09:00 - 17:59	Online MUD - EvilMog	
09:00 - 17:59	The Schemaverse Championship	
09:00 - 17:59	Wireless Capture the Flag	
09:00 - 17:59	Io57 Mystery Challenge	
09:00 - 17:59	OSINTSECCryptoAIBlockchain	
09:00 - 17:59	Social Engineer SECTF4Teens	
10:00 - 19:59	DEF CON Scavenger Hunt	
10:00 - 13:59	SOHOpelessly Broken CTF	
13:00 - 14:30	Film Festival: Project Immerse: A Deepfake Paranoi . . .	
18:00 - 19:59	No Tech Talks	
18:00 - 19:59	Hacker Jeopardy	
18:30 - 19:59	Film Festival: Project Immerse: A Deepfake Paranoi . . .	
20:00 - 21:59	Whose Slide is It Anyway	
Sunday		
00:00 - 11:59	TeleChallenge	
00:00 - 15:59	ULTIMATE Secure Coding Throwdown (Secure Code Warr . . .	
00:00 - 15:59	Io57 Mystery Challenge	
00:00 - 15:59	OSINTSECCryptoAIBlockchain	
00:00 - 15:59	Social Engineer SECTF4Teens	
06:00 - 15:59	SEATF: Maritime Hacking CTF	
09:00 - 17:59	AppSec Village CTF	
09:00 - 17:59	Be the Match - registration drive	
09:00 - 17:59	Bio-Hacking - Hospital Under Siege	
09:00 - 17:59	Capture The Packet (CTP)	
09:00 - 17:59	Car Hacking Village CTF	
09:00 - 17:59	CMD+CTRL CyberRange	
09:00 - 17:59	Crack Me If You Can (CMIYC)	

PDT Times	Title	speaker
09:00 - 11:59	Darknet Contest	
09:00 - 17:59	(Before Con) Creative Writing Short Story Contest	
09:00 - 17:59	Coindroids	
09:00 - 17:59	The Gold Bug – Crypto and Privacy Village Puzzle	
09:00 - 17:59	Hackfortress	
09:00 - 17:59	H@cker Runw@y	
09:00 - 17:59	HomebrewHardware Contest	
09:00 - 17:59	ICS Hack the Plan[e]t	
09:00 - 17:59	Defcon Ham Radio Fox Hunting Contest	
09:00 - 11:59	OpenSOC Blue Team CTF - Finals Round	
09:00 - 17:59	Online MUD - EvilMog	
09:00 - 17:59	The Schemaverse Championship	
09:00 - 17:59	Wireless Capture the Flag	
10:00 - 11:59	DEF CON Scavenger Hunt	
10:00 - 13:59	SOHOpelessly Broken CTF	

[Return to Index](#)

Crypto & Privacy Village

Friday: 10:00 - 18:00 , Saturday: 10:00 - 18:00 , Sunday: 10:30 - 13:00

Location: [#cpv-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:59	STARTTLS is Dangerous	Hanno Böck
11:00 - 11:59	LadderLeak: Breaking ECDSA With Less Than One Bit . . .	Akira Takahashi,F. Novae . . .
12:00 - 12:59	The Norwegian Blue: A lesson in Privacy Engineerin . . .	Eivind Arvesen
13:00 - 13:59	Dos, Donts and How-Tos of crypto building blocks u . . .	Mansi Sheth
14:00 - 14:59	How to store sensitive information in 2020?	Mansi Sheth
15:00 - 15:59	Workshop: Let's Talk About Abusability Testing	Avi Zajac,Francesca Spek . . .
16:00 - 16:59	DNS Privacy	Matt Cheung
17:00 - 17:59	Fireside Chat: All about Section 230, the EARN IT . . .	Cathy Gellis,Riana Pfeffe . . .
Saturday		
10:00 - 10:59	Quantum Computers & Cryptography	I. Shaheem
11:00 - 11:30	Online Ads as a Recon and Surveillance Tool	Neil M
11:30 - 11:59	Who needs spyware when you have COVID-19 apps? A 1 . . .	C. Nadal,J. DeBlois,M. . . .
12:00 - 12:59	Differential Privacy..more important than ever in . . .	Aditi Joshi
13:00 - 13:59	Rights You Can't Exercise Can't Protect You: P . . .	Ben Brook,Maritza Johnson . . .
14:00 - 14:59	Hacking like Paris Hilton 14 years later - and sti . . .	Per Thorsheim
15:00 - 15:59	Online Voting: Theory and Practice	Emily Stamm,Porter Adams
16:00 - 16:59	Next level stalker ware	Cecilie Wian
17:00 - 17:59	Workshop: Let's Talk About Abusability Testing	Avi Zajac,Francesca Spek . . .
Sunday		
10:30 - 10:59	European regulatory trends for Artificial Intellig . . .	Julia Reinhardt
11:00 - 11:30	Fear, Uncertainty, and Doubt about Human Microchip . . .	Zhanna Malekos Smith
11:30 - 11:59	What if we had TLS for phone numbers? An introduct . . .	Kelley Robinson
12:00 - 12:59	Workshop: Let's Talk About Abusability Testing	Avi Zajac,Francesca Spek . . .
13:00 - 13:30	File Encryption For Actual Humans	David Kane-Parry

[Return to Index](#)

Career Hacking Village

Friday: 1000 - 1800, Saturday: 1000 - 1800

Location: [#cahv-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:59	From Barista to Cyber Security Pro, Breaking the E . . .	Alyssa Miller
11:00 - 11:59	But I Still Need A Job!	Kirsten Renner
12:00 - 12:59	Hacking Security Leadership	Pete Keenan
13:00 - 13:59	Key Ingredients for the Job Interviews (Virtual or . . .	Roy Wattanasin
14:00 - 14:59	Pwning Your Resume	Kris Rides
15:00 - 15:59	In theory, there is no difference between theory a . . .	Pablo Breuer
16:00 - 16:59	Building Teams in the New Normal	Mike Murray
17:00 - 17:59	Future Proofing Your Career	Jenai Marinkovic
Saturday		
10:00 - 10:59	Cons and Careers	Steven Bernstein
11:00 - 11:59	The Individual Contributor to Tech Executive, or T . . .	Amelie Koran
12:00 - 12:59	Entrepreneurial Adventures: What It Takes to Start . . .	Bryson Bort
13:00 - 13:59	National Service Panel: Career Opportunities Suppo . . .	John Felker,Diane Janosek . . .
14:00 - 14:59	Veteran Transition Tips	Bob Wheeler
15:00 - 15:59	Drinks with Recruiters	Kris Rides,Rachel Bozeman . . .

[Return to Index](#)

DEFCON Talk Tracks
Location: [#track-1-live](#)
Location: [#track-1-live-qa](#)

PDT Times	Title	speaker
Thursday		
09:30 - 09:59	Discovering Hidden Properties to Attack Node.js ec ...	Feng Xiao
10:30 - 10:59	Room for Escape: Scribbling Outside the Lines of T ...	Alvaro Munoz,Oleksandr Mi ...
11:30 - 11:59	DNSSECTION: A practical attack on DNSSEC Zone Walk ...	Hadrien Barral,Rémi Gér ...
12:30 - 12:59	Hacking the Hybrid Cloud	Sean Metcalf
13:30 - 13:59	Hacking traffic lights	Rik van Duijn,Wesley Neel ...
14:30 - 14:59	Hacking the Supply Chain – The Ripple20 Vulnerab ...	Ariel Schön,Moshe Kol,Sh ...
15:30 - 15:59	Demystifying Modern Windows Rootkits	Bill Demirkapi
16:30 - 16:59	Domain Fronting is Dead, Long Live Domain Fronting ...	Erik Hunstad
Friday		
09:30 - 09:59	Welcome to DEF CON Safe Mode	The Dark Tangent
10:30 - 10:59	Spectra—New Wireless Escalation Targets	Francesco Gringoli,Jiska ...
11:30 - 11:59	Pwn2Own Qualcomm compute DSP for fun and profit	Slava Makkaveev
12:30 - 12:59	Detecting Fake 4G Base Stations in Real Time	Cooper Quintin
13:30 - 13:59	When TLS Hacks You	Joshua Maddux
14:30 - 14:59	Finding and Exploiting Bugs in Multiplayer Game En ...	Jack Baker
15:30 - 15:59	Don't Be Silly - It's Only a Lightbulb	Eyal Itkin
16:30 - 16:59	Exploiting Key Space Vulnerabilities in the Physic ...	Bill Graydon
17:30 - 17:59	A Hacker's guide to reducing side-channel attack ...	Elie Bursztein
18:30 - 18:59	Office Drama on macOS	Patrick Wardle
Saturday		
09:30 - 09:59	A Decade After Stuxnet's Printer Vulnerability: Pr ...	Peleg Hadar,Tomer Bar
10:30 - 10:59	Whispers Among the Stars: Perpetrating (and Preven ...	James Pavur
11:30 - 11:59	Don't Ruck Us Again - The Exploit Returns	Gal Zror
12:30 - 12:59	Applied Ca\$h Eviction through ATM Exploitation	Brenda So,Trey Keown
13:30 - 13:59	How we recovered \$XXX,000 in Bitcoin from an encry ...	Michael Stay
14:30 - 14:59	Abusing P2P to Hack 3 Million Cameras: Ain't Nobod ...	Paul Marrapese
15:30 - 15:59	Bypassing Biometric Systems with 3D Printing and E ...	Yamila Levalle
16:30 - 16:59	Reverse Engineering the Tesla Battery Management S ...	Patrick Kiley
17:30 - 17:59	Getting Shells on z/OS with Surrogat Chains	Jake Labelle
20:00 - 21:59	Movie Stream - Lost World	
Sunday		
09:30 - 09:59	Evil Printer: How to Hack Windows Machines with Pr ...	Chuanda Ding,Zhipeng Huo
10:30 - 10:59	Bytes In Disguise	Jesse Michael,Mickey Shka ...
11:30 - 11:59	Only takes a Spark - Popping a shell on a 1000 nod ...	ayoul3
14:30 - 14:59	Beyond Root: Custom Firmware for Embedded Mobile C ...	Christopher Wade

PDT Times	Title	speaker
15:30 - 15:59	Practical VoIP/UC Hacking Using Mr.SIP: SIP-Based . . .	Ismail Melih Tas,Kubilay . . .
16:30 - 16:59	Lateral Movement and Privilege Escalation in GCP; . . .	Allison Donovan,Dylan Ayr . . .
17:00 - 17:59	Closing Ceremonies	The Dark Tangent

[Return to Index](#)

DEFCON Groups

Location: [#dcg-stage-voice](#)

PDT Times	Title	speaker
Saturday		
10:00 - 10:59	OWASP API Top 10	
11:00 - 11:59	Government Espionage on a School Lunch Budget	
12:00 - 12:59	Basic OSINT: Mining Personal Data	
13:00 - 13:15	Intro to DC858	
13:15 - 13:59	Saving Yourself from Microsoft: It's by design	
14:00 - 14:59	Understanding the Threat: Malicious Software, Mali . . .	
15:00 - 15:15	Intro to DC603	
15:15 - 15:59	DNS New World Order, version 1.4: QuadX! DoH! DoT! . . .	
17:00 - 17:59	Introducing Melbourne DCG by Allen and Friends	
Sunday		
15:00 - 15:59	DEF CON Groups Panel	Brent White / B1TK1LL3R,C . . .

[Return to Index](#)

DEFCON Demo Labs

Each DemoLab has a Discord Channel. Check the [DC28 DemoLabs](#) page for more info.

PDT Times	Title	speaker
Friday		
10:00 - 11:50	Carnivore (Microsoft External Attack Tool)	Chris Nevin
10:00 - 11:50	CIRCO v2: Cisco Implant Raspberry Controlled Opera . . .	Emilio Couto
12:00 - 13:50	PyRDP: Remote Desktop Protocol Monster-in-the-Midd . . .	Olivier Bilodeau
12:00 - 13:50	Mobile Security Framework - MobSF	Ajin Abraham
14:00 - 15:50	jeopardize	Utku Sen
16:00 - 17:55	redlure	Matthew Creel
Saturday		
10:00 - 11:50	jeopardize	Utku Sen
10:00 - 11:50	Starkiller	Vincent “Vinnybod Ro . . .
12:00 - 13:50	Phirautee	Viral Maniar
14:00 - 15:50	PyRDP: Remote Desktop Protocol Monster-in-the-Midd . . .	Olivier Bilodeau,Alexandr . . .
16:00 - 17:55	CIRCO v2: Cisco Implant Raspberry Controlled Opera . . .	Emilio Couto
16:00 - 17:55	Cotopaxi: IoT Protocols Security Testing Toolkit	Jakub Botwicz
Sunday		
10:00 - 11:50	redlure	Matthew Creel
10:00 - 11:50	MalConfScan with Cuckoo	Tomoaki Tani,Shusei Tomon . . .
12:00 - 13:50	Carnivore (Microsoft External Attack Tool)	Chris Nevin
12:00 - 13:50	Starkiller	

[Return to Index](#)

[Entertainment](#)

Check the [DC28 Entertainment](#) page for more info.

PDT Times	Title	speaker
Friday		
18:00 - 18:59	Terrestrial Access Network	
19:00 - 19:59	Acid T	
20:00 - 20:59	Icetre Normal	
21:00 - 21:59	Zebbler Encanti Experience	
22:00 - 22:59	Ninjula	
23:00 - 23:59	Shadowvex	
Saturday		
18:00 - 18:59	tense future	
19:00 - 19:59	Mica Husky	
20:00 - 20:59	Dj St3rling	
21:00 - 21:59	Skittish & Bus	
22:00 - 22:59	Miss Jackalope	
23:00 - 23:59	Subxian	

[Return to Index](#)

Ethics Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#ev-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Federal Communications Commission	Comm. Geoffrey Starks
12:00 - 12:59	U.S. Privacy and Civil Liberties Oversight Board M . . .	Travis LeBlanc
14:00 - 14:59	Models of Privacy Norms	R. Jason Cronk,Ece Gumuse . . .
16:00 - 16:59	Security of Election Systems: A contract case stud . . .	Rim Boujnah
Saturday		
10:00 - 10:59	Killer Robots Reconsidered	Diane Vavrichek,Larry Lew . . .
12:00 - 14:10	Vote @ Home Workshop	Andrea Matwyshyn
14:10 - 15:20	Federal Trade Commision	Comm. Rohit Chopra
15:20 - 16:30	Food and Drug Administration	Jessica Wilkerson
16:30 - 17:40	TechCongress	Leisel Bogan
Sunday		
10:00 - 10:59	Blackmail, Extortion and the Ethics of Disclosure	Michael Antonino
12:00 - 12:59	How to Start a Movement: Hackers Edition	Chloé Messdaghi
14:00 - 14:59	Open Live Chat for all Speakers or another talk on . . .	Ethics Village Staff

[Return to Index](#)

Fireside Lounge

Location: [#fireside_lounge-voice](#)

PDT Times	Title	speaker
Friday		
20:00 - 20:59	D0 N0 H4RM: A Healthcare Security Conversation	Ash Luft,Christian “qua . . .
21:00 - 21:59	Shrek, Juggs, and Toxic Trolls: a BADASS discussio . . .	Katelyn Bowden,Rachel Lam . . .
Saturday		
19:00 - 19:59	Ask the EFF/Meet the EFA	Abi Hassen,Alexis Hancock . . .

[Return to Index](#)

Hardware Hacking Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#hhv-infobooth-text](#)

PDT Times	Title	speaker
Friday		
09:30 - 09:59	Meetup: Some HHV Challenges	rehr
10:00 - 10:30	Learn to Solder the BadgeBuddy Kit	Joseph Long (hwbxr)
11:00 - 11:59	Hardware hacking 101: There is plenty of room at t . . .	Federico Lucifredi
12:30 - 12:59	onkeypress=hack();	Farith Pérez Sáez,Luis . . .
13:30 - 14:30	HackerBox 0057 Build Session	Joseph Long (hwbxr)
14:30 - 14:59	Meetup: PCB Proto and Rework	ShortTie
15:30 - 15:59	Meetup: Legacy Hardware	ShortTie
17:30 - 17:59	Meetup: Some HHV Challenges	rehr
18:00 - 18:59	Meetup: 3H: Hardware Happy Hour	Chris Gammell
Saturday		
08:30 - 08:59	Learn to Solder the BadgeBuddy Kit	Joseph Long (hwbxr)
09:30 - 09:59	Hardware hacking 101: There is plenty of room at t . . .	Federico Lucifredi
11:00 - 11:30	onkeypress=hack();	Farith Pérez Sáez,Luis . . .
12:00 - 12:30	Learn to Solder the BadgeBuddy Kit	Joseph Long (hwbxr)
13:00 - 13:30	Meetup: Some HHV Challenges	rehr
14:00 - 14:30	Meetup: Sourcing Parts	bombnav
15:00 - 15:30	Meetup: OSS ASIC	Josh Marks
16:00 - 16:30	Meetup: Certification Processes (UL, FCC, etc.)	ShortTie
Sunday		
09:00 - 09:30	Learn to Solder the BadgeBuddy Kit	Joseph Long (hwbxr)
10:00 - 10:30	Meetup: Sourcing Parts	bombnav
11:30 - 12:30	HackerBox 0057 Build Session	Joseph Long (hwbxr)
12:30 - 12:59	Meetup: Wearables	ShortTie
13:00 - 13:59	Importing vector graphics in to EagleCAD	
14:00 - 14:30	Learn to Solder the BadgeBuddy Kit	Joseph Long (hwbxr)

[Return to Index](#)

[Ham Radio Village](#)

Village: Friday: 10:00 - 16:00, Saturday: 10:00 - 16:00, Sunday: 10:00 - 14:00

Exams: Friday: 11:00 to 17:00, Saturday: 14:00 to 17:00, Sunday: 15:00 to 17:00

PDT Times	Title	speaker
Friday		
10:00 - 10:15	Village Opening Remarks	
11:00 - 13:59	Ham Radio USA License Exams (Friday)	
11:00 - 11:59	Talking to Satellites	
13:00 - 13:30	A Basic Ham Station Setup	
14:00 - 14:59	So You Got an SDR: Common Signals and the Wiki	
Saturday		
10:00 - 10:59	Single Board Computers in Amateur Radio	
11:30 - 12:30	Discussion: What makes a good ham radio operator?	
13:30 - 13:59	Practice 'Net' via Discord	
14:00 - 16:59	Ham Radio USA License Exams (Saturday)	
15:00 - 15:30	OSTWERK Initiative	
Sunday		
10:00 - 11:30	The K0BAK Rover Van	
13:00 - 13:30	APRS: Automatic Packet Reporting System Demo	
14:30 - 14:45	Village Closing Commentary	
15:00 - 17:59	Ham Radio USA License Exams (Sunday)	

[Return to Index](#)

[Hack the Sea Village](#)

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#htsv-general-text](#)

PDT Times	Title	speaker
Thursday		
13:00 - 13:59	Dockside with the US Coast Guard	
Friday		
10:00 - 10:30	Yacht PWNed	Stephen Gerling
12:00 - 12:59	Build a Raspberry AIS	Dr. Gary Kessler
14:00 - 14:59	40,000 Leagues UUV Death Match	Dr. Nina Kollars
Saturday		
10:00 - 10:59	Speed 2: The Poseidon Adventure – When Cruise Sh . . .	Andrew Tierney
11:00 - 11:59	Hack the SeaPod	Grant Romundt
Sunday		
11:00 - 11:59	Hack the SeaPod	Fathom5

[Return to Index](#)

Industrial Control Systems Village

Friday: 09:00-18:00, Saturday: 09:00-18:00, Sunday: 09:00-12:00

Location: [#ics-general-text](#)

PDT Times	Title	speaker
Friday		
09:00 - 09:59	Keynote	Chris Krebs
10:15 - 10:45	ICS Village CTF Kick-Off	Tom
11:00 - 11:30	Mission Kill: Process Targeting in ICS Attacks	Joe Slowik
11:45 - 12:15	Vulnerability Discovery - Tips for Surviving and T...	Dor Yardeni, Mike Lemley
12:30 - 13:30	On the insecure nature of turbine control systems ...	Alexander Korotin, Radu Mo...
13:45 - 14:45	The Journey of ICS Project Files - Visibility and ...	Nadav Erez
15:00 - 15:30	5 Quick Wins for Improving your ICS Cybersecurity ...	Austin Scott
15:45 - 16:45	PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS	Ben Gardiner
Saturday		
09:00 - 09:30	ICS SecOps: Active Defense Concept with Effective ...	
09:45 - 10:45	Confessions of an Offensive ICS Cyber Security Res ...	Marina Krotofil
11:00 - 11:59	Playing with Electricity: Hacking into Distributio ...	Can Demirel, Serkan Temel
12:15 - 13:15	Vivisecting PowerPC	ac0rn, atlas 0f d00m
13:30 - 13:59	MITRE ICS ATT&CK	Marie, Otis
14:15 - 15:15	Building a Physical Testbed for Blackstart Restora ...	Tim Yardley
15:30 - 16:30	Operationalizing Cyber Norms: Critical Infrastruct ...	Chris Kubecka
16:45 - 17:15	Industrial Cybersecurity in Mexico	Octavio Fernandez, Victor ...

[Return to Index](#)

Internet of Things Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-12:30

Location: [#iotv-general-text](#)

PDT Times	Title	speaker
Friday		
09:15 - 09:45	How to get rights for hackers	Chloé Messdaghi
10:00 - 10:30	IoT Hacking Stories in Real Life	Besim Altinok
10:45 - 11:45	Getting Started – Building an IoT Hardware Hacki . . .	
12:15 - 12:59	Exploring vulnerabilities in Smart Sex Toys, the e . . .	Denise Giusto Bilic
13:15 - 13:59	IoT Under the Microscope: Vulnerability Trends in . . .	Parker Wiksell
14:15 - 14:59	Hella Booters: Why IoT Botnets Aren't Going Anywhe . . .	Netspooky
15:15 - 16:15	NAND Flash – Recovering File Systems from Extrac . . .	
16:45 - 17:30	Assembling VULNtron: 4 CVEs that Turn a Teleconfer . . .	Mark Bereza
17:45 - 18:15	Pandemic In Plaintext	Troy Brown
18:30 - 19:15	The Joy of Coordinating Vulnerability Disclosure	Daniel Gruss,CRob,Lisa Br . . .
Saturday		
09:00 - 09:45	Hacking smart-devices for fun and profit: From exp . . .	Barak Sternberg
10:00 - 10:45	Your connected world isn't yours anymore! - Remote . . .	Dewank Pant,Shruti Lohani
11:00 - 11:59	Introduction to U-Boot Interaction and Hacking	Garrett Enoch
12:30 - 13:15	Kicking Devices and Taking CVEs : The Zoomer's G . . .	Sanjana Sarda
13:45 - 14:15	In search of the perfect UPnP tool	Trevor Stevado t1v0
14:30 - 15:20	The future of IoT Security “Baselines, Stand . . .	Amit Elazari,Anahit Tarkh . . .
15:30 - 16:30	Learning to Use Logic Analyzers	Jonathan Stines
17:00 - 17:45	IoT Honeypots and taming Rogue appliances	Kat Fitzgerald
18:00 - 18:45	Stepped on a Nail	Matthew Byrdwell

[Return to Index](#)

Lock Bypass Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#lbv-social-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 11:30	Bypass 101 + Q&A	
11:30 - 12:59	DIY Bypass Tool Workshop + Q&A	
13:00 - 14:59	General Q&A / Drop-in and Chat	
15:00 - 16:30	Alarm Bypass + Q&A	
16:30 - 16:59	General Q&A / Drop-in and Chat	
Saturday		
11:00 - 12:30	Bypass 101 + Q&A	
12:30 - 13:59	Alarm Bypass + Q&A	
14:00 - 15:30	Reconnaissance + Q&A	
15:30 - 16:59	Bypass 101 + Q&A	
Sunday		
11:00 - 12:30	Bypass 101 + Q&A	
14:00 - 15:30	DIY Bypass Tool Workshop + Q&A	
15:30 - 16:59	General Q&A / Drop-in and Chat	

[Return to Index](#)

Lock Pick Village

Friday: 09:00-18:00, Saturday: 09:00-18:00, Sunday: 09:00-17:00

Location: [#lpv-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Intro to Lockpicking	The Open Organisation Of ...
11:00 - 11:50	Key Duplication - It's not just for the movies!	Tony Virelli
12:00 - 12:30	Intro to Lockpicking	The Open Organisation Of ...
13:00 - 13:30	Hybrid PhySec tools - best of both worlds or just ...	d1dymu5
14:15 - 14:45	Intro to Lockpicking	The Open Organisation Of ...
15:00 - 15:30	Doors, Cameras, and Mantraps OH MY!	Dylan The Magician
16:15 - 16:45	Intro to Lockpicking	The Open Organisation Of ...
Saturday		
10:00 - 10:30	Intro to Lockpicking	The Open Organisation Of ...
10:45 - 11:45	High Security Wafer Locks - An Oxymoron?	zeefeene
12:00 - 12:30	Intro to Lockpicking	The Open Organisation Of ...
13:00 - 13:45	Law School for Lockpickers	Preston Thomas
14:15 - 14:45	Intro to Lockpicking	The Open Organisation Of ...
15:00 - 15:59	Bobby Pins, More Effective Than Lockpicks?	John the Greek
16:15 - 16:45	Intro to Lockpicking	The Open Organisation Of ...
17:00 - 17:59	Intro to high security locks and lockpicking	N thing
Sunday		
10:00 - 10:30	Intro to Lockpicking	The Open Organisation Of ...
11:00 - 11:50	Safecracking for Everyone!	Jared Dygert
12:00 - 12:30	Intro to Lockpicking	The Open Organisation Of ...
13:00 - 13:30	Keystone to the Kingdom	Austin Marck
14:15 - 14:45	Intro to Lockpicking	The Open Organisation Of ...
15:00 - 15:59	How I defeated the Western Electric 30c	N thing
16:15 - 16:45	Intro to Lockpicking	The Open Organisation Of ...

[Return to Index](#)

Monero Village

Thursday: 09:00-18:00, Friday: 09:00-18:00, Saturday: 09:00-18:00, Sunday: 09:00-17:00

Location: [#mv-general-text](#)

PDT Times	Title	speaker
Friday		
09:50 - 09:59	Welcome Speech	rehr
10:00 - 11:30	Keynote: Monero: Sound Money Safe Mode	Dr. Daniel Kim
12:00 - 12:30	Proposed Mitigation Measures to Address a Disrupti . . .	Dr. Francisco "ArticMine" . . .
13:00 - 13:59	This year's village badge	Michael Schloh von Bennew . . .
14:30 - 15:30	Getting started with the Intervillage badge	Michael Schloh von Bennew . . .
15:30 - 15:59	Monero Wallet Basics: Sending, Receiving, Proving	rehr
16:00 - 16:59	Meme Competition	
Saturday		
10:00 - 11:30	Keynote: Monero: Sound Money Safe Mode	Dr. Daniel Kim
12:00 - 12:59	Open Office Q&A w/ Monero Research Lab's Sarang	Sarang
13:30 - 14:30	Badge Clinic	Michael Schloh von Bennew . . .
15:00 - 15:30	Decentralization in a Centralized world	rehr
16:00 - 16:30	Tricky Bundles: Smarter Dependency Management for . . .	idk
16:30 - 16:59	Kahoot! Quiz	
Sunday		
10:00 - 11:30	Keynote: Monero: Sound Money Safe Mode	Dr. Daniel Kim
12:00 - 12:30	You're not the money printer, or why we need to se . . .	sgp
13:00 - 13:30	Locha Mesh: Monero off-the-grid	Randy Brito
13:30 - 14:30	Badge Clinic	Michael Schloh von Bennew . . .
15:30 - 15:59	Closing talk	rehr

[Return to Index](#)

Payment Village

Friday: 10:00-14:00, Saturday: 10:00-14:00, Sunday: 10:00-14:00

Location: [#pay-labs-text](#)

PDT Times	Title	speaker
Friday		
09:45 - 09:59	Welcome to the Payment Village	Leigh-Anne Galloway
10:00 - 10:59	Making sense of EMV card data – decoding the TLV . . .	Dr Steven J. Murdoch
11:00 - 11:59	Fear and Loathing in Payment Bug Bounty	Timur Yunusov
Saturday		
10:00 - 10:59	Identity Crisis: the mad rise of online account op . . .	Uri Rivner
11:00 - 11:59	Online Banking Security	Arkadiy Litvinenko
12:00 - 12:59	Trends in the online card payment security	Dr Mohammed Aamir Ali
Sunday		
10:00 - 10:59	PoS Terminal Security Uncovered	Aleksei Stennikov
11:00 - 11:59	Architecting Modern Payment Gateways in .Net core . . .	Menaka BaskerPillai

[Return to Index](#)

Packet Hacking Village Talks

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#phv-infobooth-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Media Analysis of Disinformation Campaigns	Chet Hosmer, Mike Raggo
13:00 - 13:59	Dumpster Fires: 6 Things About IR I Learned by Bei . . .	Dr. Catherine Ullman
16:00 - 16:59	Take Down the Internet! With Scapy	C8 (John Hammond)
Saturday		
10:00 - 10:59	The Vulnerability That Gmail Overlooked and Enabli . . .	Özkan Mustafa Akkus
13:00 - 13:59	The Worst Mobile Apps	Sam Bowne
Sunday		
11:00 - 11:59	Packet Acquisition: Building the Haystack	Chris Abella, Pete Anderso . . .

[Return to Index](#)

Packet Hacking Village Workshops

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#phv-infobooth-text](#)

PDT Times	Title	speaker
Friday		
13:00 - 14:59	Intrusion Analysis and Threat Hunting with Open So . . .	Jack Mott,Jason Williams, . . .
16:00 - 17:59	Violent Python 3	Elizabeth Biddlecome,Irvi . . .
Saturday		
09:00 - 10:59	Writing Wireshark Plugins for Security Analysis	Jeswin Mathai,Nishant Sha . . .
13:00 - 14:59	Wireshark for Incident Response & Threat Hunting	Michael Wylie
16:00 - 17:59	Advanced APT Hunting with Splunk	Matt Toth,Robert Wagner
Sunday		
09:00 - 12:59	Bad Active Directory (BAD)	Dhruv Verma,Michael Rober . . .

[Return to Index](#)

[Policy Village](#)

Friday: 09:00-17:00, Saturday: 9:00-17:00, Sunday: 10:00-12:00

Location: [#pol-general-text](#)

PDT Times	Title	speaker
Friday		
15:30 - 16:30	Election Security	
Saturday		
11:00 - 11:59	AMA w/@hackingdave & @kennwhite	hackingdave,kennwhite
14:00 - 14:59	AMA w/Polycymakers	
16:00 - 16:59	Mis/Dis Information & Democracy	

[Return to Index](#)

Password Village

Friday: 09:00-18:00, Saturday: 9:00-18:00, Sunday: 09:00-14:00

Location: [#pwdv-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Getting Started with Hashcat	Password Village Staff
13:00 - 13:30	Making Targeted Wordlists	Password Village Staff
15:00 - 15:30	Result of Longer Passwords in Real World Applicati . . .	Minga
16:00 - 16:59	From Printers to Silver Tickets or Something	EvilMog
18:00 - 18:59	Getting Advanced with Hashcat	Password Village Staff
21:00 - 21:30	Getting Started with Hashcat (Rebroadcast)	Password Village Staff
21:30 - 21:59	Making Targeted Wordlists (Rebroadcast)	Password Village Staff
22:00 - 22:30	Result of Longer Passwords in Real World Applicati . . .	Minga
22:30 - 22:40	From Printers to Silver Tickets or Something (Rebr . . .	EvilMog
22:40 - 23:30	Getting Advanced with Hashcat (Rebroadcast)	Password Village Staff
Saturday		
00:00 - 00:59	PathWell: Dynamic Password Strength Enforcement (R . . .	Hank Leininger
10:00 - 10:59	Cracking at Extreme Scale: The Evolution of Hashst . . .	Jeremi M Gosney (epixoip)
12:00 - 12:59	What the Shuck? Layered Hash Shucking	Sam Croley (Chick3nman)
13:00 - 13:59	PathWell: Dynamic Password Strength Enforcement	Hank Leininger
14:00 - 14:59	Practical PCFG Password Cracking	Matt Weir
21:00 - 21:59	Cracking at Extreme Scale: The Evolution of Hashst . . .	Jeremi M Gosney (epixoip)
22:00 - 22:59	Length 15 & No Change. Implementing NIST SP800-63B . . .	Per Thorsheim
23:00 - 23:59	What the Shuck? Layered Hash Shucking (Rebroadcast . . .	Sam Croley (Chick3nman)
Sunday		
01:00 - 01:59	Practical PCFG Password Cracking (Rebroadcast)	Matt Weir

[Return to Index](#)

Recon Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#rv-general-text](#)

PDT Times	Title	speaker
Saturday		
10:00 - 10:30	Twitter Word Phrequency	Master Chen
11:00 - 11:30	Burnout is real	Chloé Messdaghi
12:00 - 12:30	Hunting for Blue Mockingbird Coinminers	Ladislav B
13:00 - 13:45	Ambly, the Smart Darknet Spider	Levi
14:00 - 14:30	COVID 1984_ Propaganda and Surveillance during a P . . .	Mauro Cáseres

[Return to Index](#)

Rogue's Village

Friday: 10:00-18:00, Saturday: 10:00-18:00, Sunday: 10:00-14:00

Location: [#rov-announcements-text](#)

PDT Times	Title	speaker
Friday		
11:00 - 11:59	Rogues Village Introduction	Rogues Village Team
12:00 - 13:59	Google Maps Hacks	Simon Weckert
14:00 - 14:59	Performance	Daniel Roy
16:00 - 17:59	Pickpocketing @ Home	James Harrison
Saturday		
14:00 - 14:59	Performance	Daniel Roy
16:00 - 17:59	Outs, Forces, and Equivoque: A treatise on how Ma . . .	Brandon Martinez
Sunday		
12:00 - 13:59	Rogues adventure & the intervillage badge	Monero Village Team,Rogue . . .

[Return to Index](#)

Red Team Offense Village

Thursday: 07:00 - 24:00, Friday: 24hrs, Saturday: 24hrs, Sunday: until 17:00

Location: #rtv-briefings-text

PDT Times	Title	speaker
Thursday		
07:30 - 07:59	Red Team Village Announcements and Remarks	Joseph Mlodzianowski (c . . .
08:00 - 08:59	The Bug Hunter's Methodology	Jason Haddix
09:00 - 08:59	Red Team Village CTF - Prequal	
09:15 - 10:15	Securing AND Pentesting the Great Spaghetti Monste . . .	Kat Fitzgerald
10:30 - 11:30	Guerrilla Red Team: Decentralize the Adversary	Christopher Cottrell
11:45 - 12:45	Evil Genius: Why you shouldn't trust that keyboard	Farith Perez, Mauro Cáser . . .
13:00 - 13:59	Combining notebooks, datasets, and cloud for the u . . .	Ryan Elkins
14:15 - 15:15	Deep Dive into Adversary Emulation - Ransomware Ed . . .	Jorge Orchilles
15:30 - 16:30	Introducing DropEngine: A Malleable Payload Creati . . .	Gabriel Ryan
16:45 - 17:45	Zero Trust - A Vision for Securing Cloud and Redef . . .	Vandana Verma Sehgal
18:00 - 18:59	What college kids always get wrong, the art of att . . .	Forrest Fuqua
19:15 - 20:15	Android Malware Adventures	Kürşat Oğuzhan Akınc. . .
20:30 - 21:30	Making Breach and Attack Simulation Accessible and . . .	Shay Nehmad
21:45 - 22:45	Android Application Exploitation	Kyle Benac (aka @B3nac)
23:00 - 23:59	Offensive Embedded Exploitation : Getting hands di . . .	Kaustubh Padwad
Friday		
07:30 - 07:59	Red Team Village Opening Remarks	Joseph Mlodzianowski (c . . .
08:00 - 08:59	Knock knock, who's there? Identifying assets in th . . .	Tanner Barnes (aka @_Stat . . .
09:30 - 15:59	Red Team Village CTF - Finals	
09:15 - 10:15	Red Teaming: Born from the Hacker Community	Chris Wysopal
10:30 - 11:30	Panel: The Joy of Coordinating Vulnerability Discl . . .	Daniel Gruss, CRob, Lisa Br . . .
11:45 - 12:45	How to hack SWIFT, SPID, and SPEI with basic hacki . . .	Guillermo Buendia
13:00 - 13:59	Trust, but Verify: Maintaining Democracy In Spite . . .	Allie Mellen
14:15 - 15:15	Grey Hat SSH: SShenanigans	Evan Anderson
15:30 - 16:30	Yippee-Ki-Yay MFA'er - Bypassing Multi-Factor Auth . . .	Justin Hutchens ("Hutch . . .
16:45 - 17:45	Enumerating Cloud File Storage Gems	Michael Wylie
18:00 - 18:59	Total E(A)gression	Alvaro Folgado Rueda
19:15 - 20:15	Password cracking beyond 15 characters and under \$. . .	Travis Palmer
20:30 - 21:30	50 Shades of Sudo Abuse	Tyler Boykin
21:45 - 22:45	ATTPwn: Adversarial Emulation and Offensive Techni . . .	Fran Ramirez, Pablo Gonzal . . .
23:00 - 23:59	ERPwnage - a red team approach to targeting SAP	Austin Marck
Saturday		
01:00 - 01:59	Back to the future: Computer science and systems b . . .	Dr Lorenz Adlung, Noa Novo . . .
02:15 - 03:15	Modern Red Team Tradecraft - Informing Defenders b . . .	Sajal Thomas
03:30 - 04:30	Executing Red Team Scenarios with Built-in Scenari . . .	Erdener Uyan, Gökberk Gü . . .
04:45 - 05:45	OU having a laugh?	Petros Koutroumpis

PDT Times	Title	speaker
06:00 - 06:59	All of the threats: Intelligence, modelling and hu . . .	Tim Wadhwa-Brown
07:15 - 08:15	Catch Me if You Can	Eduardo Arriols
08:30 - 09:30	Mechanizing the Methodology: Automating Discovery, . . .	Daniel Miessler
09:45 - 10:45	Y'all Tryna Bypass Python 3.8 Audit Hooks or Nah?	Leron Gray
11:00 - 11:59	Initial Compromise through Web Side	Walter Cuestas
12:15 - 12:30	Inside the Mind of a Threat Actor: Beyond Pentesti . . .	Phillip Wylie
12:45 - 13:45	The Student Roadmap to Becoming A Penetration Test . . .	Jonathan Helmus
14:15 - 14:59	The Art of Balancing: A Burnout Talk	Chloé Messdaghi
15:15 - 16:15	APTs <3 PowerShell and Why You Should Too	Anthony Rose,Jake "Hubb . . .
16:30 - 17:30	Indicators of Emulation: Extra Spicy Adversary Emu . . .	Ch33r10,haydnjohnson
17:45 - 18:45	Emulating an Adversary with Imperfect Intelligence	Adam Pennington
19:00 - 19:59	Automating Threat Hunting on the Dark Web and othe . . .	Apurv Singh Gautam
20:15 - 21:15	Bypassing in Mobile Network From Red-Team Points o . . .	Ali Abdollahi
21:30 - 22:30	Sounds Legit: Why you shouldn't trust that speaker	Luis Ángel Ramírez Mend . . .
22:45 - 23:59	Weaponized XSS - Moving Beyond Alert(1)	Ray Doyle
Sunday		
01:00 - 01:59	PatrOwl - Red flavour of SOC automation	Nicolas MATTIOCCO
02:15 - 03:15	Reviewing MS08-067, Illustration Of An Old Chapter	Etizaz Mohsin
03:30 - 04:30	RedTeamOps - Managing Red Team Infrastructure as a . . .	Mert Can Coşkuner
04:45 - 05:45	From Discovery to Disclosure	Ibad Shah
06:00 - 06:59	Hacking Zoom: a Hacker's Journey into Zoom Securit . . .	Mazin Ahmed
07:15 - 08:15	PWN The World	Chris Kubecka
08:30 - 09:30	Autonomous Security Analysis and Penetration Testi . . .	Ankur Chowdhary
09:45 - 10:45	Kubernetes Goat - Vulnerable by Design Kubernetes . . .	Madhu Akula
11:00 - 11:59	Breaking the Attack Chain	Corey Ham,Matt Eidelberg
12:15 - 13:15	Hashes; Smothered, Covered, and Scattered: Modern . . .	Lee Wangenheim
13:30 - 14:30	You're Adversary Within - The Golden Age of Inside . . .	Adam Mashinchi
15:00 - 15:59	Have my keys been pwned? - API Edition	José Hernandez,Rod Soto
16:00 - 16:59	Red Team Village Closing Ceremony and Announcement . . .	Joseph Mlodzianowski (c . . .

[Return to Index](#)

[Social Engineering Village](#)

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#sev-general-text](#)

PDT Times	Title	speaker
-----------	-------	---------

Friday

13:00 - 13:59 [Live SE Q&A](#)

[Return to Index](#)

Voting Machine Hacking Village

Friday: 10:00-17:00, Saturday: 10:00-17:00, Sunday: 10:00-14:00

Location: [#vmhv-general-text](#)

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Welcome and Kick-Off	Harri Hursti,Matt Blaze,M . . .
10:30 - 10:59	Keynote Remarks: Representative Jackie Speier	Jackie Speier
11:00 - 11:30	A Policy Approach to Resolving Cybersecurity Probl . . .	Jody Westby
11:30 - 12:30	Hacking Democracy II: On Securing an Election Unde . . .	Casey John Ellis,Kimber D . . .
12:30 - 12:59	See Something, Say Something	Marten Mickos
13:00 - 13:59	A Panel with the Feds on Election Security	Bryson Bort,David Imbordi . . .
14:00 - 14:30	Keynote Remarks: Senator Ron Wyden	Ron Wyden
14:30 - 14:59	Chairman Benjamin Hovland, US Election Assistance . . .	Benjamin Hovland
15:00 - 15:30	Secretary Kim Wyman, Washington	Kim Wyman
20:00 - 20:59	Live Q&A with Special Guests Regarding "Kill Chain . . .	
Saturday		
10:00 - 10:30	War By Other Means: How Influence Operations Under . . .	Ben Dubow
10:30 - 10:59	John Odum, Montpelier, VT	John Odum
11:00 - 11:30	Heightened Election Security Risks Admist the Pand . . .	Jack Cable,Alex Zaheer
11:30 - 11:59	Hack-a-Fax	Forrest Senti,Mattie Gull . . .
12:00 - 12:30	Analysis of the Attack Data Collected During Mobil . . .	Nimit Sawhney,Nailah Mims
12:30 - 12:59	Remote Online Balloting Delivery and Marking Optio . . .	Susan Greenhalgh,Steve Ne . . .
13:00 - 13:30	Don't Go Postal Over Mail In Voting	Bianca Lewis
13:30 - 13:59	The Ballot is Busted Before the Blockchain: A Secu . . .	Michael A. Specter
14:00 - 14:30	Vote-from-home? Review of Election Security on Rem . . .	Sang-Oun Lee
14:30 - 14:59	Electronic Ballot Return Standards & Guidelines	Forrest Senti,Mattie Gull . . .
15:30 - 15:59	A Lawyer's Reflections on Elections	Cordero Alexander Delgadi . . .
15:00 - 15:30	Understanding Cyber-Attacks and Their Implications . . .	Javier F. Patiño García
16:00 - 16:30	Protecting Elections with Data Science -- A Tool f . . .	Stephanie Singer

[Return to Index](#)

Wireless Village

Friday: 09:00-19:00, Saturday: 09:00-19:00, Sunday: 09:00-17:00

Location: [#wv-general-text](#)

PDT Times	Title	speaker
Thursday		
09:00 - 09:01	wicked wardriving with gps and glonass	wytshadow
09:00 - 09:01	Introduction to WiFi Security	Nishant Sharma
09:00 - 09:01	Wireless Blue Team	Eric Escobar
09:00 - 09:01	DragonOS - How I kept busy during COVID19	cemaxecuter
09:00 - 09:01	The Basics Of Breaking BLE v3	FreqyXin
Friday		
17:45 - 18:45	Wireless Village Fireside Talk	
Sunday		
12:00 - 12:59	Ghosting the PACS-man: New Tools and Techniques	Iceman,Omikron

[Return to Index](#)

Talk/Event Descriptions



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON

AIV - Saturday - 09:30-09:59 PDT

Title: "SECRETS ARE LIES, SHARING IS CARING, PRIVACY IS THEFT." - A Dive into Privacy Preserving Machine Learning

When: Saturday, Aug 8, 09:30 - 09:59 PDT

Where: AI Vlg

SpeakerBio: Nahid Farhady

No BIO available

Description: No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: (Before Con) Creative Writing Short Story Contest

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The DEF CON Short Story contest is a pre-con contest that is run entirely online utilizing the DEF CON forums and subreddit. This contest follows the theme of DEF CON for the year and encourages hackers to roll up their sleeves and write the best creative story that they can. The Short Story Contest encourages skills that are invaluable in the hacker's world, but are sometimes overlooked. Creative writing in a contest setting helps celebrate creativity and originality in arenas other than hardware or software hacking and provides a creative outlet for individuals who may not have another place to tell their stories.

Forum: <https://forum.defcon.org/node/231200>

Discord: <https://discord.com/channels/708208267699945503/711643275584340069>

Twitter: <https://twitter.com/dcshortstory>

Return to Index - Add to  - ics [Calendar](#) file

Title: (Before Con) Creative Writing Short Story Contest

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The DEF CON Short Story contest is a pre-con contest that is run entirely online utilizing the DEF CON forums and subreddit. This contest follows the theme of DEF CON for the year and encourages hackers to roll up their sleeves and write the best creative story that they can. The Short Story Contest encourages skills that are invaluable in the hacker's world, but are sometimes overlooked. Creative writing in a contest setting helps celebrate creativity and originality in arenas other than hardware or software hacking and provides a creative outlet for individuals who may not have another place to tell their stories.

Forum: <https://forum.defcon.org/node/231200>

Discord: <https://discord.com/channels/708208267699945503/711643275584340069>

Twitter: <https://twitter.com/dcshortstory>

Return to Index - Add to  - ics [Calendar](#) file

Title: (Before Con) Creative Writing Short Story Contest

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The DEF CON Short Story contest is a pre-con contest that is run entirely online utilizing the DEF CON forums and subreddit. This contest follows the theme of DEF CON for the year and encourages hackers to roll up their sleeves and write the best creative story that they can. The Short Story Contest encourages skills that are invaluable in the hacker's world, but are sometimes overlooked. Creative writing in a contest setting helps celebrate creativity and originality in arenas other than hardware or software hacking and provides a creative outlet for individuals who may not have another place to tell their stories.

Forum: <https://forum.defcon.org/node/231200>

Discord: <https://discord.com/channels/708208267699945503/711643275584340069>

Twitter: <https://twitter.com/dcshortstory>

Return to Index - Add to  - ics [Calendar](#) file

Title: 10,000 Dependencies Under The Sea: Exploring and Securing Open source dependencies

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: AppSec Vlg

Speakers: Gregg Horton, Ryan Slama

SpeakerBio: Gregg Horton

No BIO available

Twitter: [@greggawatt](#)

SpeakerBio: Ryan Slama

No BIO available

Description:

Come on our journey of creating scalable tooling and processes to automatically identify vulnerabilities in third-party libraries and handle the question of “ok we found this, who’s going to fix it?”

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: 21 Jump Server: Going Bastionless in the Cloud

When: Saturday, Aug 8, 12:30 - 13:15 PDT

Where: Cloud Vlg

SpeakerBio: Colin Estep

Colin Estep is currently a threat researcher at Netskope focused on AWS and GCP. Colin was previously the CSO at Sift Security (acquired by Netskope), where he helped move the product towards breach detection for IaaS. He was a senior engineer on the security teams at Netflix and Apple before joining Sift. He was also a FBI Agent specializing in Cyber crime, where he spent a fair amount of time coordinating with other countries to locate and arrest malware authors and botnet operators.

Twitter: [@colinestep](https://twitter.com/colinestep)

Description:

If you are a customer of AWS, Azure, or GCP, you may have deployed your own bastion hosts to provide RDP or SSH access to your virtual machines. While bastions help to protect your infrastructure, there are challenges that come along with them, such as managing the identities, obtaining logs, and preventing SSH multiplexing attacks.

In this talk, we will briefly review bastion hosts and some of their shortcomings, as well as the SSH multiplexing attack. The SSH multiplexing attack uses a feature of SSH to pivot from a compromised laptop to your bastion hosts. From there, the attacker could use this feature to compromise other users and gain access to your virtual machines hosted in the cloud.

Finally, we'll show you services that provide access to your virtual machines in all three major cloud providers that eliminate the need for bastion hosts. Some providers have more than one alternative. However, this presentation will not present all of the alternatives. It is focused on the services that generally take the following approach:

Users authenticate to the access service with their Identity and Access Management (IAM) credentials for the cloud provider. Once authenticated, the cloud service creates an encrypted tunnel with port forwarding, which runs SSH or RDP for the user.

The benefits of this approach include:

Public IP addresses are not required in order to access the virtual machines. It eliminates the possibility of compromising an entire organization with SSH multiplexing attacks. In some cases, disabling a user's IAM credentials also removes SSH or RDP access. Cloud audit logs will capture metadata for RDP or SSH sessions, and in some cases, full session logs are easy to collect through the provider's service. We'll cover Session Manager in AWS, OS Login and Identity-Aware Proxy (IAP) in GCP, and the Bastion Service in Azure. You'll see how the services work, how they help with identity management, and where to find the SSH sessions in logs. If you are migrating to any of these platforms, this could save you from having to go through the pain of deploying your own solutions!

YouTube: https://www.youtube.com/watch?v=gwBG_oKDINQ

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: 2FA in 2020 and Beyond

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: AppSec Vlg

SpeakerBio: Kelley Robinson

Kelley works on the Account Security team at Twilio. Previously she worked in a variety of API platform and data engineering roles at startups. Her research focuses on authentication user experience and design trade-offs for different risk profiles and 2FA channels. Kelley lives in Brooklyn, is an avid home cook, and spends too much time on Twitter (@kelleyrobinson).

Twitter: [@kelleyrobinson](https://twitter.com/kelleyrobinson)

Description:

Security professionals agree: SMS based Two-factor Authentication (2FA) is insecure, yet thousands of companies still employ this method to secure their customer-facing applications. This talk will look at the evolution of authentication and provide a data-driven analysis of the tradeoffs between the different types of factors available.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HTS - Friday - 14:00-14:59 PDT

Title: 40,000 Leagues UUV Death Match

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Hack the Sea VIg

SpeakerBio:Dr. Nina Kollars

No BIO available

Description:No Description available

Hack the Sea Village activities will be streamed to Twitch.

Twitch: <https://twitch.tv/hackthesea>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Friday - 15:00-15:30 PDT

Title: 5 Quick Wins for Improving your ICS Cybersecurity Posture

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: ICS Vlg

SpeakerBio: Austin Scott

With 18 years of industrial automation experience, Austin Scott (GICSP, CISSP, OSCP) is a Principal Industrial Penetration Tester at Dragos Inc., where he identifies cyber risk within industrial control networks. Before Dragos, Austin worked as part of the OT cybersecurity team at Sempra, Shell, and as an industrial cybersecurity consultant at Accenture. Austin is a SANS Cybersecurity Difference Maker (2015) winner for his industrial cybersecurity contributions. Austin has won the DEFCON UBER black badge and has also published three books on PLC programming.

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - [ics Calendar file](#)

RTV - Friday - 20:30-21:30 PDT

Title: 50 Shades of Sudo Abuse

When: Friday, Aug 7, 20:30 - 21:30 PDT

Where: Red Team Vlg

SpeakerBio: Tyler Boykin

Tyler Boykin is a former 0602 (USMC), hobbyist infosec geek, and is a Security Engineer with By Light Professional IT Services LLC currently developing features for CyberCENTS (a By Light Offering). He currently holds a variety of industry credentials to include OSCE, OSCP, CISSP, CCNP, CCDP, and many others.

Description:

Privilege escalation often includes abusing pre-existing features on a system. This talk gives a quick overview of sudo, sudoers, and ways of leveraging misconfigurations to increase access. Included in this talk, are vectors that range from common low-hanging fruit to downright crafty.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar](#) file

BCV - Saturday - 15:00-15:59 PDT

Title: 7 Phases of Smart Contract Hacking

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: Blockchain VIg

SpeakerBio: Martin Abbatemarco

No BIO available

Description: No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: 747 Walkthrough From A Hacker's Perspective

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: Aerospace Vlg

Speakers: Alex Lomas, Ken Munro

SpeakerBio: Alex Lomas

Alex Lomas is Pen Test Partner's aerospace specialist. Alex undertakes penetration testing of traditional IT, such as networks, web applications, and APIs, as well as more aviation-specific areas including airport operational technology and avionics embedded systems such as inflight entertainment and e-enabled aircraft.

SpeakerBio: Ken Munro

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 Aviation Village, the Global Connected Aircraft Summit, and the Aviation ISAC Summit among others.

Description:

This will be a tour of an end of life 747 airframe, covering a 101 of the cockpit systems and avionics bays. We will also be explaining the various systems & threat surfaces.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Friday - 13:00-13:30 PDT

Title: A Basic Ham Station Setup

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: Ham Radio Vlg

Description:

In this live demo, we'll go over a basic home ham radio station setup, including all of the components and how they work together.

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: A Decade After Stuxnet's Printer Vulnerability: Printing is still the Stairway to Heaven

When: Saturday, Aug 8, 09:30 - 09:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Peleg Hadar, Tomer Bar

SpeakerBio: Peleg Hadar , Security Researcher at SafeBreach Labs

Peleg Hadar (@peleghd) is a security researcher, having 8+ years of unique experience in the sec field. Currently doing research @SafeBreach Labs, previously serving in various sec positions @IDF.

His experience involved security from many angles: starting with network research, and now mostly software research. Peleg likes to investigate mostly Microsoft Windows components.

Twitter: [@peleghd](https://twitter.com/peleghd)

SpeakerBio: Tomer Bar , Research Team Leader at SafeBreach Labs

Tomer Bar is a security researcher and a research team leader with 15+ years of unique experience in the sec field. Currently leading the research team of SafeBreach Labs.

His experience involved vulnerability research, malware analysis, etc.

Description:

In 2010, Stuxnet, the most powerful malware in the world revealed itself, causing physical damage to Iranian nuclear enrichment centrifuges. In order to reach Iran's centrifuges, it exploited a vuln in the Windows Print Spooler service and gain code execution as SYSTEM. Due to the hype around this critical vuln, we (and probably everyone else) were pretty sure that this attack surface would no longer exist a decade later. We were wrong...

The first clue was that 2 out of 3 vulns which were involved in Stuxnet were not fully patched. That was the case also for the 3rd vuln used in Stuxnet, which we were able to exploit again in a different manner. It appears that Microsoft has barely changed the code of the Print Spooler mechanism over the last 20 years. We investigated the Print Spooler mechanism of Windows 10 Insider and found two 0-day vulns providing LPE and DoS (First one can also be used as a new persistence technique)

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Deeper Dive Into ILS And ADS-B Spoofing

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: Aerospace VIg

SpeakerBio:Harshad Sathaye

Harshad is a Ph.D. candidate at Northeastern University and a soon-to-be student pilot. He is a cyber security enthusiast with research interests around wireless systems security, specifically navigation systems and development of secure cyber-physical systems

Description:

Modern aircraft heavily rely on several wireless technologies for communications control and navigation. Researchers demonstrated vulnerabilities in many aviation systems e.g., spoofing ILS signals to disrupt the landing, injecting ghost aircraft into airspace, spoof locations, and manipulate key communication messages. This presentation will give the viewers a better understanding of the fundamental problems associated with these critical systems and what makes spoofing attacks possible.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Hacker's guide to reducing side-channel attack surfaces using deep-learning

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Elie Bursztein , Google

Elie Bursztein leads Google' security & anti-abuse research team. He has authored over fifty research papers in the field for which he was awarded 8 best papers awards and multiple industry distinctions including the Black Hat pwnie award. Born in Paris, he received a Ph.D. from ENS-cachan in 2008 before working at Stanford University and ultimately joining Google in 2011.

Twitter: [@elie](#)

Description:

in recent years, deep-learning based side-channel attacks have been proven to be very effective and opened the door to automated implementation techniques. Building on this line of work, this talk explores how to take the approach a step further and showcases how to leverage the recent advance in AI explainability to quickly assess which parts of the implementation is responsible for the information. Through a concrete set by step example, we will showcase the promise of this approach, its limitations, and how it can be used today.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Sunday - 11:00-11:45 PDT

Title: A Heaven for Hackers: Breaking a Web Security Virtual Appliances

When: Sunday, Aug 9, 11:00 - 11:45 PDT

Where: AppSec Vlg

SpeakerBio: Mehmet D. Ince

No BIO available

Twitter: [@mdisec](#)

Description: No Description available

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: A Lawyer's Reflections on Elections

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: Voting VIg

SpeakerBio: Cordero Alexander Delgadillo , Attorney, Sublime Law, PLLC

No BIO available

Twitter: [@CORDERO_ESQ](#)

Description:

Join Cordero Alexander Delgadillo (@CORDERO_ESQ), a business and technology lawyer, and more recently a former political candidate, as he demonstrates that elections, especially local elections, are akin to information systems (even reasonably locked down systems), because both are highly susceptible to the very non-tech, human vulnerabilities (nefarious and negligent). In this talk Cordero will provide insight by:

- Examining the structures of American Democracy
- Telling stories from his own election lawsuit: Delgadillo v. City of Peoria et al
- Highlighting election process issues deemed “inconsequential” or “un-addressable”
- Sharing information and resources

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A N00b's Intro to Building Your Own Lab (Beginner)

When: Saturday, Aug 8, 16:30 - 17:59 PDT

Where: Blue Team VIg - Workshop Track 2

SpeakerBio: Omar Santos , Cisco

Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure. Omar is the author of over 20 books and video courses; numerous white papers, and other articles. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities. Omar is often presenting at many conferences and he is the co-lead of the DEF CON Red Team Village.

Twitter: [@santosomar](#)

Description:

This is a brief introduction of how to build your own virtualized, physical, or cloud-based environment to practice your skills in a safe ecosystem. Create a lab for offensive and defensive cybersecurity concepts. You will also learn and obtain access to numerous tools that you can use to practice your skills, from virtual machines (VMs), Docker containers, and intentionally vulnerable systems. Using tools like Proxmox or even OpenStack to build your own cyber range. In addition, you will also learn how to use tools like Vagrant and Ansible to automate a lot of tasks.

Numerous cybersecurity, malware analysis, and penetration testing tools and techniques have the potential to damage or destroy the target system or the underlying network. In addition, if malware is used in testing, there is the potential for infection and spread if testing in an Internet-connected testbed. This is a brief introduction (beginners and intermediate) were you will learn how to build your own virtualized, physical, or cloud-based environment to practice your skills in a safe ecosystem.

You will learn what you need to do to create a lab for offensive and defensive cybersecurity concepts. You will also learn and obtain access to numerous tools that you can use to practice your skills, from virtual machines (VMs), Docker containers, and intentionally vulnerable systems. You will learn how you can leverage tools like Proxmox, or even OpenStack to build your own cyber range. In addition, you will also learn how to use tools like Vagrant and Ansible to automate a lot of tasks. Vagrant files and Ansible playbooks will be shared during the class for you to build complex lab environments within minutes. We will also go over a few demos on how to create environments in cloud services such as AWS, Azure, Google Cloud, and Digital Ocean.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Panel with the Feds on Election Security

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Voting Vlg

Speakers: Bryson Bort, David Imbordino, Brig. Gen. William Hartman, Matthew Masterson, Cynthia Kaiser, Dan Kimmage

SpeakerBio: Bryson Bort

Founder of SCYTHE, next generation attack emulation platform; GRIMM, cybersecurity consultancy; ICS Village Co-Founder, 501c3 for ICS security awareness. Senior Fellow for Cyber/National Security at R Street and National Security Institute; Advisor to the Army Cyber Institute and DHS/CISA.

SpeakerBio: David Imbordino , Election Security Lead, National Security Agency

No BIO available

SpeakerBio: Brig. Gen. William Hartman , Commander, Cyber National Mission Force

No BIO available

SpeakerBio: Matthew Masterson , Senior Cybersecurity Advisor, CISA

No BIO available

SpeakerBio: Cynthia Kaiser , Deputy Chief of Analysis for National Security Cyber Threats, FBI

No BIO available

SpeakerBio: Dan Kimmage , Principal Deputy Coordinator, Global Engagement Center, Department of State

No BIO available

Description:

Elections are critical in a free and fair society. Public trust in election infrastructure begins with understanding what the Government has done with transparency and how the hacker community can help. We are all citizens and our voices should be heard.

- What has the Federal Government done since 2016 including with state and local?
- What changes have come about with the military's Defend Forward strategy in 2018?
- How do they work together with the domestic efforts?
- How are foreign and domestic campaigns of disinformation managed?
- What else could we do better?
- How can the hacker community help?

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A Policy Approach to Resolving Cybersecurity Problems in the Election Process

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: Voting VIg

Speaker Bio: Jody Westby, CEO, Global Cyber Risk LLC

No BIO available

Description:

Cybersecurity researchers keep identifying cybersecurity vulnerabilities in voting machines and in the election process, but not much happens in closing identified vulnerabilities. The private sector vendors involved in voter registration, manufacturing and programming voting machines, and vote tabulation are less than responsive and few have not provided evidence that they have strong cybersecurity programs that meet best practices and standards and regularly have cyber risk assessments performed. This presentation will put forward a federal policy approach that will help correct these problems and advance the integrity of elections across the country.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A View From The Cockpit: Exploring Pilot Reactions To Attacks On Avionic Systems

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: Aerospace VIg

SpeakerBio: Matt Smith

Matt is a Postdoctoral Research Associate in the System Security Lab led by Prof. Ivan Martinovic, at the Department of Computer Science, University of Oxford. His research looks at the security of wireless systems in aviation, most recently focusing on the impacts of attacks on safety systems. Prior to this, Matt completed his PhD in the Department of Computer Science, University of Oxford, covering avionic data links and the effects of attacks in the cockpit. He holds a Masters degree in Computer Science from the University of Warwick.

Description:

Researchers have been crafting attacks on aviation systems for almost a decade now, on wireless technologies like ADS-B and ACARS to In Flight Entertainment (IFE) devices. Many attacks seek to affect what the pilots see or how the aircraft is flown. Although we can work out what should happen in theory, does this translate to practice? In this talk, we describe how we investigated this using a flight simulator and 30 type-rated commercial pilots.

In particular, we will discuss:

- What happens when your aircraft thinks you are on collision course - but nothing is there, - How pilots respond when landing guidance puts you at the wrong end of the runway (i.e. the reverse Die Hard), - Can attackers push flight crew into switching systems off?

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

Return to Index - Add to  - ics [Calendar](#) file

Title: A-ISAC CTF

When: Saturday, Aug 8, 08:00 - 19:59 PDT

Where: Aerospace Vlg

Description:

Aviation is under attack! A Tier 1 airport is in chaos!

Ticketing kiosks, airline servers, flight information displays, transportation security, runway lights, aircraft, and other critical systems have all been compromised. And there are indicators that airport insiders may have colluded with hackers to bring the airport to its knees!

It's up to you now. YOU have 24 hours to research and investigate this crisis to regain control of the targeted airport and its airspace. From collecting evidence (and flags) to restoring all compromised assets and assisting impacted stakeholders, the clock is ticking!

Its time to apply everything you know about cybersecurity (e.g., password cracking, log analysis, computer forensics, and ethical hacking), intelligence (e.g., OSINT), and aviation (e.g., crew, avionics, air traffic control communications, airline operations, security screening, airport information systems, and aviation cyber-physical systems) to help the airport return to normal operations.

You have been given full authority to do whatever it takes to catch the hackers, seize back control of the airport, and restore aviation operations.

Discord: <https://discord.com/channels/708208267699945503/734477413186273400>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: A-ISAC CTF

When: Friday, Aug 7, 08:00 - 19:59 PDT

Where: Aerospace Vlg

Description:

Aviation is under attack! A Tier 1 airport is in chaos!

Ticketing kiosks, airline servers, flight information displays, transportation security, runway lights, aircraft, and other critical systems have all been compromised. And there are indicators that airport insiders may have colluded with hackers to bring the airport to its knees!

It's up to you now. YOU have 24 hours to research and investigate this crisis to regain control of the targeted airport and its airspace. From collecting evidence (and flags) to restoring all compromised assets and assisting impacted stakeholders, the clock is ticking!

Its time to apply everything you know about cybersecurity (e.g., password cracking, log analysis, computer forensics, and ethical hacking), intelligence (e.g., OSINT), and aviation (e.g., crew, avionics, air traffic control communications, airline operations, security screening, airport information systems, and aviation cyber-physical systems) to help the airport return to normal operations.

You have been given full authority to do whatever it takes to catch the hackers, seize back control of the airport, and restore aviation operations.

Discord: <https://discord.com/channels/708208267699945503/734477413186273400>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Abusing P2P to Hack 3 Million Cameras: Ain't Nobody Got Time for NAT

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Paul Marrapese , Security Researcher

Paul Marrapese (OSCP) is a security researcher from San Jose, CA. His work has resulted in the discovery of critical vulnerabilities affecting millions of IoT devices around the world, and has been featured on Krebs on Security, Forbes, Wired, ZDNet, and several security podcasts. Paul specializes in offensive security as part of the red team at a large enterprise cloud company. His interests include reverse engineering, music production, photography, and recently software-defined radio. Rumor has it that he makes a mean batch of cold-brew coffee.

Twitter: [@PaulMarrapese](#)

Description:

To a hacker, making a bug-ridden IoT device directly accessible to the Internet sounds like an insanely bad idea. But what's *truly* insane is that millions of IoT devices are shipping with features that expose them to the Internet the moment they come online, even in the presence of NAT and firewalls. P2P, or “peer-to-peer”, is a convenience feature designed to make the lives of users easier, but has the nasty side effect of making attackers’ lives easier as well.

Come for the story of how supply chain vulnerabilities in modern IP cameras, baby monitors, and even alarm systems are putting millions at risk for eavesdropping and remote compromise. We'll talk about the hoards of IoT devices that exist outside of Shodan's reach and the botnet-like infrastructure they rely on. Learn how to find P2P networks and how to exploit them to jump firewalls, steal camera passwords over the Internet, and correlate devices to physical addresses. We'll demonstrate how to snoop on someone's video simply by using your own camera – and how someone may be snooping on your video, too.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

Return to Index - Add to  - ics [Calendar](#) file

ENT - Friday - 19:00-19:59 PDT

Title: Acid T

When: Friday, Aug 7, 19:00 - 19:59 PDT

Where: See Description or Village

Description:

DEF CON 28 may be cancelled, but our parties cannot be stopped! Tune in for a massive virtual party that will shake the NET

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Twitch: https://www.twitch.tv/defcon_music

Facebook: <https://www.facebook.com/dj.sm0ke>

Twitter: https://twitter.com/DJ_Sm0ke

YouTube: <https://www.youtube.com/channel/UC55xsENb9PKz-IKB5zodYGA/featured>

SoundCloud: https://soundcloud.com/acid_t

[Return to Index](#) - Add to  - ics [Calendar](#) file

CHV - Friday - 10:00-10:59 PDT

Title: Adding new features by manipulating CAN bus

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Car Hacking Vlg 001

SpeakerBio: Teejay

No BIO available

Description:

Overview of how I added a front camera to my vehicle last year by utilizing CAN

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUej1Q&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Advanced APT Hunting with Splunk

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: Packet Hacking VIg - Workshop

Speakers: Matt Toth, Robert Wagner

SpeakerBio: Matt Toth , Security Strategist, Splunk

Matt Toth is a Security Strategist at Splunk with over 20 years of experience in the Information Technology industry, with a focus on Cyber Security. Working with the US Department of Defense, he has led teams in CyberWar simulations, and has advised senior leadership on new attack vectors and threat actors.

SpeakerBio: Robert Wagner , Security Strategist

Robert Wagner is a security professional with 20+ years of InfoSec experience. He is a co-founder of "Hak4Kidz.com", an organizer with Burbsec and BurbSecCon in Chicago, and is on the Board of Directors of the ISSA Chicago Chapter.

Description:

You wanna learn how to hunt the APTs? This is the workshop for you. Using a real-worldish dataset, this workshop will teach you how to hunt the "fictional" APT group Taedonggang. We discuss the Diamond model, hypothesis building, LM Kill Chain, and Mitre ATT&CK framework and how these concepts can frame your hunting. Using Splunk and OSINT, we will hunt for APT activity riddling a small startup's network. During the event, you will be presented a hypothesis and conduct your own hunts, whether it is for persistence, exfiltration, c2 or other adversary tactics. Heck, there might be some PowerShell to be found, too. We will regroup and review the specific hunt and discuss findings and what opportunities we have to operationalize these findings as well. At the end, we give you a dataset and tools to take home and try newly learned techniques yourself.

This workshop requires registration. If you are registered, please proceed to #phv-infobooth-text and you'll be given access to join.

#phv-infobooth-text: <https://discord.com/channels/708208267699945503/708242376883306526>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Advancing Medical Device Security – How collaboration between providers, manufacturers, and pen testers is advancing what’s possible with security.

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: BioHacking Vlg

SpeakerBio: Mitchell Parker

Mitchell Parker is the CISO of a \$6.5B integrated delivery network (IU Health) that runs 17 hospitals and hundreds of clinics, and is responsible for securing the networks that the devices which support them live on. He is also a vice chair of IEEE P2733, Trust, Integrity, Privacy, Protection, Safety, and Security for the Internet of Medical Things.

Description:

This panel features five industry folks working toward improving medical device security through multiple channels and methods and discussing how provider, vendor, and security collaborations are leading toward significant improvements in medical device security.

These panelists and moderator represent the organizations working to actively collaborate between the independent researchers, device vendors, information security officers, clinical engineering, electronic medical records vendors, and security companies with a goal of continual improvement. These 5 represent part of a significantly larger effort, and have contributed to open standards.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Aerospace Village Badge

When: Saturday, Aug 8, 09:30 - 09:59 PDT

Where: Aerospace Vlg

SpeakerBio: Rick Hansen

Professor Rick Hansen teaches cybersecurity and IoT at Capitol Technology University. He performs original research in vulnerability assessment for embedded systems and telecommunications. Rick also serves as the CEO of APS Global llc which provides cybersecurity, research, and training to government and industry. Rick is an Air Force veteran with degrees in computer science and electronic engineering. He volunteers with Capitol's Astronautical Engineering program, assisting students with payloads operating in near-space and low-earth orbit. Professor Hansen was honored to be featured in this year's NSA Centers of Excellence in Cyber Defense video

(<https://www.capttechu.edu/student-experience/centers-and-labs/center-cybersecurity-research-and-analysis-ccra>). Last year Rick's DEFCON presentation focused on exploiting vulnerabilities in automotive LIDAR, which was the focus of this article by Unicorn Riot (<https://unicornriot.ninja/2019/hacking-lidar-changing-what-autonomous-vehicles-see/>).

Description:

Inexpensive Software-Defined Radios (SDRs) can be used to receive digital communications from aircraft and satellites. This talk presents simple experiments in receiving these communications and assessing the associated strengths and vulnerabilities. This year's Aerospace Village Badge can be used as an antenna for receiving aviation and satellite data. Materials can be purchased from Amazon and attendees will be able to follow along with the video.

This event will be coordinated on the DEF CON Discord server, in channel #av-terminal-text.

Discord: <https://discord.com/channels/708208267699945503/732392946350948423>

Return to Index - Add to  - ics [Calendar](#) file

AIV - Saturday - 15:00-15:30 PDT

Title: AI vs. Airplanes and IT-Security: What Security Regulations Teach Us About AI Governance

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: AI Vlg

SpeakerBio:Laurin Weissinger

No BIO available

Description:No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: All Aboard the CAN Bus... or Motorcycle

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Car Hacking VIg 002

SpeakerBio: Derrick (CanBusDutch)

Derrick is a corporate IT infrastructure professional, Cyber security hobbyist and motorcycle enthusiast, with more than a decade involved in the fields. When Derrick isn't consulting for major firms in the San Francisco area, feeding his autodidact addiction, or working on independent projects, he can be briefly seen as a blur passing you on the highway.

Description:

Follow me as my passion for motorcycles, goes head first into my passion for computers, and I build tools and software to reverse engineer my motorcycle's CAN system. Python scripts, microcontrollers, pulse width modulation, some potentiometers, and a bit of what I like to call "Ruthless Engineering", has helped me finally reach the pinnacle of CAN bus packet reversing. We'll cover some engine simulation, execute some packet capture session analysis, and put it all back together again, for the development of an aftermarket gauge cluster.

#chv-track002-text: <https://discord.com/channels/708208267699945503/739564953014632579>

YouTube: <https://www.youtube.com/watch?v=5DYhXbWkWoA&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack002>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: All of the threats: Intelligence, modelling and hunting through an ATT&CKers lens

When: Saturday, Aug 8, 06:00 - 06:59 PDT

Where: Red Team VIg

SpeakerBio: Tim Wadhwa-Brown

Tim Brown joined Cisco as part of their acquisition of Portcullis for whom he worked for almost 12 years. He is equally happy performing white box assessments with access to source code or where necessary diving into proprietary binaries and protocols using reverse engineering methodologies. Tim has contributed to a number of Cisco's bespoke methodologies covering subjects as diverse as risk and compliance, secure development and host hardening. Tim has looked at targets as varied as risk, mainframes, MPLS, power stations, cars, banking middleware and devops as well as supporting Cisco's SOC and incident response capability. Outside of the customer driven realm of information assurance, Tim is also a prolific researcher with papers on UNIX, KDE, Vista, Active Directory and web application security to his name. Tim is credited with almost 150 vulnerability advisories covering both kernel and userland, remote and local. Most recently Tim spoke at to the ATT&CK community on some of his use of ATT&CK for data science and threat hunting research. Tim particularly like to bug hunt enterprise UNIX solutions.

Description:

ATT&CK is a game changer and where it works, it can enable both blue and red teams to co-exist and work effectively together. However, what happens when it falls short and the threat intelligence and hypotheses don't exist? How do you build threat intelligence and threat hunt hypotheses from first principles. What do attackers on UNIX do when bitcoin miners aren't their motivation? I'll go into:

- * The target I chose and why – we have ~40 years' experience looking at UNIX from an offensive standpoint, why wouldn't attackers
- * Building a collection worksheet and the information you'll need to track
- * Figuring out what TTPs the bad guys are using to attack UNIX when no-one has documented them previously – faced with a lack of DFIR reports, how do you validate your hypotheses
- * Working out whether your customer is exposed and why this matters
- * Translating concepts we see in the wild into things our customer can consume
- * What this means for users of ATT&CK

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AMA w/@hackingdave & @kennwhite

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: See Description or Village

Speakers:hackingdave,kennwhite

SpeakerBio:hackingdave

No BIO available

Twitter: [@hackingdave](#)

SpeakerBio:kennwhite

No BIO available

Twitter: [@kennwhite](#)

Description:

This event requires registration. Please see the link below for more information.

Registration:

<https://www.eventbrite.com/e/def-con-policy-ama-ask-a-hacker-with-hackingdave-kennwhite-tickets-115981562977>

Return to [Index](#) - Add to  - ics [Calendar](#) file

POV - Saturday - 14:00-14:59 PDT

Title: AMA w/Policymakers

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: See Description or Village

Description:

This event requires registration. Please see the below link for more information.

Registration: <https://www.eventbrite.com/e/def-con-policy-ama-ask-a-policymaker-with-tbd-tickets-115983414515>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ambly, the Smart Darknet Spider

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: Recon VIg

SpeakerBio:Levi

No BIO available

Description:

Combating cybercriminal activity requires quick turnover time between detecting indicators of attack and moving to protect or remediate the malicious activity. Currently, investigations slow down at the bottleneck of manual labor required to identify and evaluate cyber threat intelligence before making an actionable decision. While this can be an issue on the Clearnet, it becomes a more difficult problem for analysts on the Darknet. This leaves cybersecurity analysts in a position of constant responsiveness, rather than endorsing a position of preemptive protection.

To minimize the need for manual labor in the triage stage of cyber threat intelligence identification and preliminary evaluation on the darknet, Ambly, a smart darknet spider, is currently under development. Utilizing this tool will help identify darknet webpages containing cyber threat intelligence and produce a report ranking webpages for further human evaluation.

Ambly is a tool designed for interacting with the Tor network, hosted by the Tor Project. By connecting to the onion routers, Ambly is able to access '.onion' URLs and begin crawling while gathering information. During the development cycle for Ambly, further layers of machine-learning modules are being added, including Natural Language Processing (NLP) classifications, language identification, and leading toward further development into cyber threat intelligence identification. This is an ongoing and dynamic research endeavor with future updates eminent. Main Talking Points:

- OSINT into CTI
- Difficulties of CTI on the Darknet
- Ambly's current abilities for intelligence gathering. - The future of Ambly and Darknet CTI.

Recon Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/c/ReconVillage>

#rv-talks-text: <https://discord.com/channels/708208267699945503/737048009732522014>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTWV2 - Saturday - 13:30-15:30 PDT

Title: An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology (Beginner)

When: Saturday, Aug 8, 13:30 - 15:30 PDT

Where: Blue Team VIg - Workshop Track 2

SpeakerBio: Ben Bornholm

No BIO available

Description:

Have you ever wondered, how should I get started in Threat Hunting? How should I start? What should I hunt for? What tools should I use? How should I do it? Have you always wanted to hunt an APT? Then this intro level workshops is the right place for you. Our workshop will introduce hunting an APT style attack to detect malicious activity at each stage of an attack's lifecycle.

This workshop will introduce you to the Attack Lifecycle model to create a fundamental framework for hunting adversaries. Our workshop will have you hunt an APT style attack to detect malicious activity at each stage of an attack's lifecycle. This will enable you to connect information found at one stage as leverage for hunting in another stage.

Participants of this workshop will have the following takeaways: - A fundamental understanding of the attacker mindset - A fundamental understanding of the phases of the Attack Lifecycle - Knowledge of the tools and techniques used by attackers - An ability to hunt for attacker tools and techniques using a SIEM - Exposure to an APT style attack - IMPORTANT: This is a 101 Intro Workshop

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTWV2 - Friday - 11:30-13:30 PDT

Title: An Introduction to Hunting Adversaries Using the Attack Lifecycle Methodology (Beginner)

When: Friday, Aug 7, 11:30 - 13:30 PDT

Where: Blue Team VIg - Workshop Track 2

SpeakerBio: Ben Bornholm

No BIO available

Description:

Have you ever wondered, how should I get started in Threat Hunting? How should I start? What should I hunt for? What tools should I use? How should I do it? Have you always wanted to hunt an APT? Then this intro level workshops is the right place for you. Our workshop will introduce hunting an APT style attack to detect malicious activity at each stage of an attack's lifecycle.

This workshop will introduce you to the Attack Lifecycle model to create a fundamental framework for hunting adversaries. Our workshop will have you hunt an APT style attack to detect malicious activity at each stage of an attack's lifecycle. This will enable you to connect information found at one stage as leverage for hunting in another stage.

Participants of this workshop will have the following takeaways: - A fundamental understanding of the attacker mindset - A fundamental understanding of the phases of the Attack Lifecycle - Knowledge of the tools and techniques used by attackers - An ability to hunt for attacker tools and techniques using a SIEM - Exposure to an APT style attack - IMPORTANT: This is a 101 Intro Workshop

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Analysis of the Attack Data Collected During Mobile Voting Pilots

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: Voting VIg

Speakers: Nimit Sawhney, Nailah Mims

SpeakerBio: Nimit Sawhney , Co-Founder and CSO, Voatz, Inc.

No BIO available

SpeakerBio: Nailah Mims , Principal Security Engineer/Analyst, Voatz, Inc.

No BIO available

Description:

Since 2018, we have been experimenting with smartphone-app based mobile voting for a very small number of voters across various jurisdictions in the United States. The small-scale nature of these pilots has not prevented attackers and researchers from around the world from attempting to break into the platform at multiple levels. In this paper, we present the significant amount of attack data that has been collected over the past couple of years and an early analysis of the nature of these attack attempts, their lethality, origins, etc. We also present the mitigation measures that have worked and the ones that haven't. Lastly, we will also dive deeper into a couple of very significant attack attempts and present a detailed analysis of the threat vectors, the attack modality, duration, etc. All this data is being shared in the public domain for the very first time and an anonymized dataset will be available for open downloads. We hope that it will further inform research in this space.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Android Application Exploitation

When: Thursday, Aug 6, 21:45 - 22:45 PDT

Where: Red Team VIg

SpeakerBio: Kyle Benac (aka @B3nac)

Kyle Benac (aka @B3nac) currently works as a full time Security Researcher at Acronis SCS. Prior to this, he obtained his Bachelors of Science in Software Development and Security while active duty Air Force. He really enjoys hacking Android applications and participating in bug bounty programs. Creator of the InjuredAndroid Capture the Flag (CTF) training application and developer of HackerOne's BountyPay Android application. Listed as a Top Contributor for the OWASP mobile security testing guide with over 58 contributions to the manual.

Twitter: [@B3nac](#)

Description:

Android applications are treasure chests of potential bugs waiting to be discovered. Having a structured, streamlined approach greatly improves your efficiency and assessment accuracy. This talk will go over methods used to identify the type of mobile framework to better assess possible attack vectors. Examples will be provided to demonstrate how to exploit those vectors.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Android Bug Foraging

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: AppSec Vlg

Speakers:João Morais,Pedro Umbelino

SpeakerBio:João Morais

No BIO available

Twitter: [@jmoraissec](#)

SpeakerBio:Pedro Umbelino

No BIO available

Twitter: [@kripthor](#)

Description:

In this session, we will analyze four real-world examples of different high impact android vulnerabilities. We will show how we discover, developed, and leveraged the vulnerabilities into a fully working proof-of-concept, devised meaningful attack scenarios (demos included), and how our work was approached by the different vendors.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Android Malware Adventures

When: Thursday, Aug 6, 19:15 - 20:15 PDT

Where: Red Team Vlg

Speakers:Kürşat Oğuzhan Akıncı,Mert Can Coşkuner

SpeakerBio:Kürşat Oğuzhan Akıncı

Kürşat Oğuzhan Akıncı is a Security Engineer at Trendyol. He is also a team leader of Blackbox Cyber Security which is Turkey's first cyber security volunteer group, coordinator and mentor of Turkcell CyberCamp and Turkish Airlines CyberTakeOff. In his free time Kürşat is performing security researches in the form of bug bounty in which he has found several vulnerabilities in critical institutions such as NSA as well as helping Mert Can to break into C&Cs.

SpeakerBio:Mert Can Coşkuner

Mert Can Coşkuner is a Security Engineer at Trendyol. He is maintaining a Penetration Testing and Malware Analysis blog at medium.com/@mcoskuner. In his free time Mert Can is performing mobile malware research and threat intelligence.

Description:

Android malware is evolving every day and they are everywhere, even in Google Play Store. Malware developers have found ways to bypass Google's Bouncer as well as antivirus solutions and many alternative techniques to operate like Windows malware do. Using benign looking application working as a dropper is just one of them. This talk is about android malware on Google Play Store and targeting Turkey. The talk will cover; Techniques to Analyze Samples: Unencrypted samples are often used to retrieve personal informations to sell and do not have obfuscation. Encrypted samples however are used for much sophisticated tasks like stealing banking information. They decrypt themselves by getting the key from a twitter account who owned by the malware developer and operate by communicating with the C&C. Also, most banking samples are using techniques like screen injection and dependency injection which is mostly used by android application developers. Bypassing Anti- Techniques: *To be able to dynamically analyze the sample, defeating anti- techniques are often needed. We will introduce some (known) Frida scripts to be able to defeat common anti- checks malware uses. Extracting IoCs: Extracting twitter account as well as C&C from encrypted samples are often critical to perform threat intelligence over samples. Extracting IoCs while assets are still active was crucial for our research since we are also aiming to takeover C&Cs. We will introduce (known) automatization technique to extract twitter account, decryption key and C&C address. 4. Extract Stolen Information from C&Cs: In order to extract information from C&C, one should act swiftly. The speed of extraction process is critical since the actors change C&Cs often. We will give a detailed walkthrough about how we approach C&Cs as a target and extract the informations. The samples and informations in the talk is the product of our researches over many bankbot samples as well as other Turkish malware developer actors' samples. Detailed talk outline*

- Google Play Store and Malware
- Common Android Malware Types
- Campaigns Aiming Turkish Users
- How To Approach An Android Malware — Techniques to Analyze
- How To Approach An Android Malware — Defeating Anti- Techniques
- How To Approach An Android Malware — Decrypting Bankbots
- How To Approach An Android Malware — IoC Extraction
- C&Cs — What Are They
- C&Cs — How To Infiltrate and Extract Information

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: API (in)Security TOP 10: Guided tour to the Wild Wild World of APIs

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: AppSec Vlg

Speakers:David Sopas,Paulo Silva

SpeakerBio:David Sopas

No BIO available

Twitter: [@dsopas](#)

SpeakerBio:Paulo Silva

No BIO available

Twitter: [@pauloasilva_com](#)

Description:

Do you speak API? Surely you do, even if you don't notice them in your world wide web everyday use. APIs are proved to be beneficial for business, but with great power comes great responsibility and some of them have serious problems. Last year we put a lot of effort to build and release the OWASP API Security Top 10 project. Then, we decided to go wild and have some fun. Now we will present our findings, from OWASP API Security Top 10 to lots of fun and profit. Join us to learn common API pitfalls: how to find and abuse them. It won't hurt. Unless your data is in there...

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8Ll0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Applied Ca\$h Eviction through ATM Exploitation

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Brenda So, Trey Keown

SpeakerBio: Brenda So , Security Researcher, Red Balloon Security

Brenda is a security researcher at Red Balloon Security. She earned her Bachelors in Electrical Engineering at The Cooper Union. She has spoken about reverse engineering at Hushcon West and CSAW. She has also organized the ATM CTF challenge at major conferences such as Recon and Defcon. When not messing around with ATMs, she is brewing a nice gallon of beer at her homebrew setup.

Twitter: [@Sosogun3](#)

SpeakerBio: Trey Keown , Security Researcher, Red Balloon Security

Trey is a security researcher at Red Balloon Security focusing on securing embedded devices and firmware reverse-engineering automation. He is the co-creator of an ATM CTF challenge which has taken place at Re:con, CSAW, Hushcon, Summercon, and the IoT Village at DEF CON 27. He has also been a speaker at Hushcon West and CSAW.

Twitter: [@TreyKeown](#)

Description:

ATMs are networked computers that dispense cash, so naturally they're uniquely interesting devices to examine. We all remember ATM jackpotting from a decade ago. Unfortunately, it doesn't look like ATM security has improved for some common models since then.

We present our reverse engineering process for working with an ATM and modifying its firmware. For this, we became our own "bank" by creating software that's able to speak the obscure protocols used by ATMs. For working with the device software at a low level, we restored JTAG access, defeated code signing, and developed custom debugging tools. We then leveraged this research to discover two 0-day network-based attacks, which we will demonstrate live. The first vulnerability takes advantage of the ATM's remote administration interface, which can lead to arbitrary code execution and total device compromise. The second vulnerability is in the OEM's implementation of a common middleware for ATM peripherals. This allows for command injection and jackpotting of ATMs over the network.

The high barrier to entry for even legally opening up one of these devices has left a lot of attack surface area unchecked. Through this talk, we want to shed light on the state of ATM security and encourage the security community to continue to challenge ATM vendors to do better.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Applying Pysa to Identify Python Security Vulnerabilities

When: Friday, Aug 7, 11:00 - 12:59 PDT

Where: AppSec Vlg

SpeakerBio: Graham Bleaney

No BIO available

Twitter: [@GrahamBleaney](https://twitter.com/GrahamBleaney)

Description:

The Product Security teams at Facebook make extensive use of static analysis to find security vulnerabilities. We use systems like Zoncolan and the open source Python Static Analyzer (Pysa) on a daily basis. Using static analysis helped us find more than 1100 security bugs in 2018, accounting for more than a third of the bugs found by the application security team in that timeframe.

In this tutorial, we'll cover the basics of static analysis, how to set up Pysa, and how you can write and run rules to identify vulnerabilities in your own codebase. We'll also cover how Pysa deals with false positives and discuss its limitations as a tool. Each new concept you learn will immediately be reinforced by a practical exercise.

Attendees should leave this tutorial with all the tools they need to start applying static analysis to their Python projects at work and in open source. A computer with Python, Pip, and Git is required for this workshop. Attendees will need to pip install pyre-check and set up a small sample project.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: AppSec Village CtF

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

CTFs test your skills, challenge your ingenuity and push mental boundaries. But what is even MORE AWESOME than a regular CTF?

A (CTF)2!! A competition that stretches your creative mind as a task author and makes you step up your game as a task player. This year, AppSec Village @ DEF CON 28 invites you to compete in both roles!

Forum: <https://forum.defcon.org/node/232292>

Discord: <https://discord.com/channels/708208267699945503/728703600586522739>

Twitter: https://twitter.com/appsec_village

Web: <https://www.appsecvillage.com/>

Return to Index - Add to  - ics [Calendar](#) file

Title: AppSec Village CtF

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

CTFs test your skills, challenge your ingenuity and push mental boundaries. But what is even MORE AWESOME than a regular CTF?

A (CTF)2!! A competition that stretches your creative mind as a task author and makes you step up your game as a task player. This year, AppSec Village @ DEF CON 28 invites you to compete in both roles!

Forum: <https://forum.defcon.org/node/232292>

Discord: <https://discord.com/channels/708208267699945503/728703600586522739>

Twitter: https://twitter.com/appsec_village

Web: <https://www.appsecvillage.com/>

Return to Index - Add to  - ics [Calendar](#) file

Title: AppSec Village CtF

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

CTFs test your skills, challenge your ingenuity and push mental boundaries. But what is even MORE AWESOME than a regular CTF?

A (CTF)2!! A competition that stretches your creative mind as a task author and makes you step up your game as a task player. This year, AppSec Village @ DEF CON 28 invites you to compete in both roles!

Forum: <https://forum.defcon.org/node/232292>

Discord: <https://discord.com/channels/708208267699945503/728703600586522739>

Twitter: https://twitter.com/appsec_village

Web: <https://www.appsecvillage.com/>

Return to Index - Add to  - ics [Calendar](#) file

HRV - Sunday - 13:00-13:30 PDT

Title: APRS: Automatic Packet Reporting System Demo

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: Ham Radio Vlg

Description:

In this live demo, we'll go over what APRS is, what you can do with it, and a quick primer on how to get started.

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: APTs <3 PowerShell and Why You Should Too

When: Saturday, Aug 8, 15:15 - 16:15 PDT

Where: Red Team VIg

Speakers:Anthony Rose,Jake “Hubbl3 Krasnov

SpeakerBio:Anthony Rose

Anthony “Cx01N Rose, CISSP, is the Chief Operating Officer of BC-Security and Lead Pentester at Mergulite Security. He has more than a decade’s worth of experience in digital communications, working with Red and Blue teams, and as an electrical engineer. His research has focused on wireless networks and embedded systems security. Anthony leveraged his research at DEF CON 24, where he published his work revealing wide-spread vulnerabilities in Bluetooth locks and brought awareness to the masses. His workshop at DEF CON 27 resulted in the reboot of the post-exploitation framework, Empire, which he actively develops and maintains.

SpeakerBio:Jake “Hubbl3 Krasnov

Jake “Hubbl3 Krasnov is the Chief Executive Officer of BC-Security. He spent the first half of his career as an aeronautical 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. His most recent focus has been on developing cybersecurity testing tools for embedded systems. He was an instructor at DEF CON 27, where he taught AMSI evasion techniques and his most recent efforts contributed to the resurrection of the post-exploitation framework Empire.

Description:

Quite often, you may have heard people mention, “Why should you bother learning PowerShell, isn’t it dead?” or “Why not just use C#? Many individuals in the offensive security field have a common misconception that PowerShell is obsolete for red team operations. Meanwhile, it remains one of the primary attack vectors employed by Advanced Persistent Threats (APTs). APTs are known for implementing sophisticated hacking tactics, techniques, and procedures (TTPs) to gain access to a system for an extended period of time. Their actions typically focus on high-value targets, which leave potentially crippling consequences to both nation-states and corporations. It is crucial that Red Teams accurately emulate real-world threats and do not ignore viable attack options. For this talk, we will walk through how many threat actors adapt and employ PowerShell tools. Our discussion begins with examining how script block logging and AMSI are powerful anti-offensive PowerShell measures. However, the implementation of script block logging places a technical burden on organizations to conduct auditing on a substantial amount of data. While AMSI is trivial to bypass for any capable adversary. Finally, we will demonstrate APT-like PowerShell techniques that remain incredibly effective against the latest generation of network defenses.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PAYV - Sunday - 11:00-11:59 PDT

Title: Architecting Modern Payment Gateways in .Net core with Azure

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: Payment Vlg

SpeakerBio: Menaka Basker Pillai

No BIO available

Description:

In this session am going to explain how to work with payment gateways and how to implement a secured payment gateways in .net core web Apps. This session also includes some core concepts of Azure that plays an important role in transaction.

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ask the EFF/Meet the EFA

When: Saturday, Aug 8, 19:00 - 19:59 PDT

Where: DEF CON Fireside Twitch

Speakers: Abi Hassen, Alexis Hancock, Elliot, Emilie St-Pierre, Eva Galperin, Hannah Zhao, Kurt Opsahl, nash, Rory Mir, Tracy Rosenberg

SpeakerBio: Abi Hassen

Abi Hassen is an attorney, technologist, and co-founder of the Black Movement-Law Project (BMLP), a legal support rapid response group that grew out of the uprisings in Ferguson, Baltimore, and elsewhere. He is currently a partner at O'Neill and Hassen LLP; a law practice focused on indigent criminal defense. Prior to his current work, he was the Mass Defense Coordinator at the National Lawyers Guild. Abi has also worked as a political campaign manager and strategist, union organizer, and community organizer. Abi conducts training, speaks, and writes on topics of race, technology, (in)justice, and the law.

SpeakerBio: Alexis Hancock

Alexis works to secure the web by working on HTTPS Everywhere. She has previously been a web developer and system administrator for 7 years and a statistician in the education realm. She has earned degrees from the Rochester Institute of Technology in Media Arts and Technology (B.Sc.) and The New School in Organizational Change Management (MS). She is very passionate about encryption and tech equity for all and has been assisting activists and educators with their tech needs for almost 10 years.

SpeakerBio: Elliot

Elliot is a motion artist and creative coder who works in interactive, fabrication, and large scale immersive experiences. Elliot blends visual work with an interest in mutual aid, security, and privacy online. Based in Brooklyn.

SpeakerBio: Emilie St-Pierre , Security Ambassador

Emilie St-Pierre is the Security Ambassador for Future Ada, a Spokane-based non-profit advocating for diversity and inclusion in STEAM. For the past six years, she has used her experience as an offensive security professional to provide privacy and security education within her community. Through her work with Future Ada, she has established free regular workshops and one-on-one technical support to the public. Emilie's focus has been to provide these workshops and services to underrepresented members of the public.

SpeakerBio: Eva Galperin , Director of Cybersecurity

Eva Galperin is EFF's Director of Cybersecurity. Prior to 2007, when she came to work for EFF, Eva worked in security and IT in Silicon Valley and earned degrees in Political Science and International Relations from SFSU. Her work is primarily focused on providing privacy and security for vulnerable populations around the world. To that end, she has applied the combination of her political science and technical background to everything from organizing EFF's Tor Relay Challenge, to writing privacy and security training materials (including Surveillance Self Defense and the Digital First Aid Kit), and publishing research on malware in Syria, Vietnam, Kazakhstan. When she is not collecting new and exotic malware, she practices aerial circus arts and learning new languages.

SpeakerBio: Hannah Zhao

Hannah is a staff attorney at EFF focusing on criminal justice and privacy issues, and is part of the Coder's Rights Project. Prior to joining EFF, Hannah represented criminal defendants on appeal in state and federal courts in New York, Illinois, and Missouri, and also worked at the human rights NGO, Human Rights in China. While pursuing her law degree at Washington University in St. Louis, she represented indigent defendants and refugee applicants in Durban, South Africa, and studied international law at Utrecht University in the Netherlands. She also competed in, and remains involved with, the Philip C. Jessup International Moot Court Competition, including as a problem author in 2019. In college, Hannah studied Computer Science and Management at Rensselaer Polytechnic Institute. In her spare time, she likes to climb things.

SpeakerBio:Kurt Opsahl , Deputy Executive Director and General Counsel, EFF

Kurt Opsahl is the Deputy Executive Director and General Counsel of the Electronic Frontier Foundation. In addition to representing clients on civil liberties, free speech and privacy law, Opsahl counsels on EFF projects and initiatives. Opsahl is the lead attorney on the Coders' Rights Project, and is representing several companies who are challenging National Security Letters. Before joining EFF, Opsahl worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters, including working on *Kelly v. Arribasoft*, *MGM v. Grokster* and *CoStar v. LoopNet*. For his work responding to government subpoenas, Opsahl is proud to have been called a "rabid dog" by the Department of Justice. Prior to Perkins, Opsahl was a research fellow to Professor Pamela Samuelson at the U.C. Berkeley School of Information Management & Systems. Opsahl received his law degree from Boalt Hall, and undergraduate degree from U.C. Santa Cruz. Opsahl co-authored "Electronic Media and Privacy Law Handbook." In 2007, Opsahl was named as one of the "Attorneys of the Year" by California Lawyer magazine for his work on the *O'Grady v. Superior Court* appeal. In 2014, Opsahl was elected to the USENIX Board of Directors.

SpeakerBio:nash

nash leads EFF's grassroots, student, and community organizing efforts. As the lead coordinator of the Electronic Frontier Alliance, nash works to support the Alliance's member organizations in educating their neighbors on digital-privacy best practices, and advocating for privacy and innovation protecting policy and legislation.

SpeakerBio:Rory Mir

Rory is a Grassroots Advocacy Organizer primarily working on the Electronic Frontier Alliance. They are also a doctoral student of psychology at the City University of New York Graduate Center studying activist pedagogy. Before coming to the EFF they were active in several New York City groups including the Cypurr Collective, a member of the EFA engaging in community education on matters of cybersecurity. A long time advocate for open education and open science, they want to break down any barriers folks face to free expression, creativity, or knowledge.

SpeakerBio:Tracy Rosenberg

Tracy Rosenberg has worked as Media Alliance's Executive Director since 2007 and coordinates Oakland Privacy, a citizens coalition that works regionally to defend the right to privacy and enhance public transparency and oversight regarding the use of surveillance techniques and equipment. OP has written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections, and community control. Tracy blogs on media policy and surveillance and is published frequently around the country. She currently sits on the board of the Alliance for Community Media Western Region and Common Frequency serves on the anchor committee of the Media Action Grassroots Network

Description:

Join the Electronic Frontier Foundation—the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age—for a candid chat about how the law is racing to catch up with technological change and discovery.

Then meet representatives from Electronic Frontier Alliance (eff.org/fight) allied community and campus organizations from across the country. These technologists and advocates are working within their communities to educate and empower their neighbors in the fight for data privacy and digital rights.

This discussion will include updates on current EFF issues such as the government's effort to compromise free expression online, the fight to end face surveillance, updates on cases and legislation affecting security research, and discussion of EFF's technology projects empowering users with greater control of what information they share online.

Half of this session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law, surveillance and technology issues that are important to you.

Discord: <https://discord.com/channels/708208267699945503/738141986476916826>

DEF CON Fireside Lounges will be live-streamed on Twitch.

Twitch: <https://www.twitch.tv/defconorg>

#fireside-lounge-text: <https://discord.com/channels/708208267699945503/738141986476916826>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Assembling VULNtron: 4 CVEs that Turn a Teleconference Robot into a Spy

When: Friday, Aug 7, 16:45 - 17:30 PDT

Where: IOT VIg

SpeakerBio:Mark Bereza

Mark Bereza is a security researcher and new addition to McAfee's Advanced Threat Research team. A recent alumnus of Oregon State's Computer Science systems program, Mark's work has focused primarily on vulnerability discovery and exploit development for embedded systems. Mark previously presented at DEFCON 27, less than 6 months after graduating college.

Description:

Once limited to the realm of science fiction, robotics now play a vital role in many industries, including manufacturing, agriculture, and even medicine. Despite this, the kind of robot that interfaces with humans directly, outside of the occasional toy or vacuum, threatens to remain an inhabitant of fiction for the foreseeable future.

temi, a “personal robot created by Roboteam, may help make that fiction a reality. temi is a smart device for consumer, enterprise, retail, and even medical environments that is capable of both autonomous movement and teleconferencing. It's precisely this functionality, however, that makes it a valuable target for hackers. Unlike a simple camera exploit, a compromised temi grants an attacker mobility in addition to audio/video, greatly increasing their ability to spy on victims in the most private of situations - their homes, medical appointments, or workplaces.

Not knowing when to quit, McAfee Advanced Threat Research uncovered four 0-day vulnerabilities in the temi. We'll show how an attacker armed with nothing besides the victim's phone number could exploit these vulnerabilities to intercept or join an existing temi call, gain video access, and even obtain “owner privileges, granting the ability to remotely control the robot – all with zero authentication.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Friday - 15:00-15:59 PDT

Title: Attacking and Defending Blockchain Nodes

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: Blockchain VIg

SpeakerBio: Peter Kacherginsky

No BIO available

Description: No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Attacking Flight Management Systems: This Is Your Captain Speaking, We Have A Small Problem!

When: Saturday, Aug 8, 08:30 - 08:59 PDT

Where: Aerospace Vlg

Speakers:Javad Dadgar,Mohammad-Reza Zamiri,Reza Dorosti

SpeakerBio:Javad Dadgar

Javad Dadgar is an independent security researcher. He is currently working as a red teamer and part-time bug bounty hunter with 4 years of experience. Also he is interested in the aviation industry.

SpeakerBio:Mohammad-Reza Zamiri

Mohammad-Reza Zamiri is a cybersecurity researcher with more than 8 years of experience. His research focuses on computer and network security, with an emphasis on detecting vulnerabilities and threats, penetration testing, as well as embedded or cyber-physical systems. He has published several research papers and presented on top conferences including (ACM CCS, ACSAC, Kaspersky) and currently is working as a senior security analyst. He also likes to play CTF and was the champion of the first national ICS CTF(2019) in Iran.

SpeakerBio:Reza Dorosti

Reza Dorosti is a software reverse engineer with more than 15 years of experience with performing dynamic analysis of software binaries and also assembly language, including x86, ARM, MIPS. He is a fan of embedded devices security.

Description:

Modern aircrafts are heavily relied on flight management systems to automate a wide variety of in-flight tasks, including producing flight plans, reducing the workload on the pilot, or allow the airplane to hook up the autopilot. Vulnerabilities in such systems could allow an attacker to manipulate critical data that are important during a flight.

In this talk, we will present the result of our research on the security of a famous flight management system and how we managed to detect a weakness in its security mechanism using reverse engineering. Then we will discuss possible risk scenarios regarding manipulation of mentioned critical data.

During this research, we have found a method to modify the navigation data on a flight management computer and also identified some risk scenarios that we think could cause some problems. We hope this may lead to future research and make the aviation industry more secure.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Attacking the Helmsman

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: Cloud Vlg

SpeakerBio: Mohit Gupta

Mohit has been a Security Consultant at F-Secure Consulting (previously known as MWR InfoSecurity) for the past four years with one of his specialisations in containerisation and orchestration technologies. Mohit leads the delivery of security services in these areas, and has been involved in a wide variety of offensive and defensive security engagements involving Docker, Docker Swarm and Kubernetes. In addition to this, he has developed and led training both externally and internally for these areas.

Twitter: [@_Skybound](#)

Description:

Kubernetes is rapidly growing in popularity and is the most popular technology for container orchestration. However, it also brings its own set of challenges and security issues which may lead to novel or unexpected attack scenarios. This talk aims to go over various areas of Kubernetes security and ways that Kubernetes features could be leveraged by an attacker. It will review the core architecture and functionality of Kubernetes from a security perspective, and cover most of the common Kubernetes security features, including Pod Security Policies, Network Policies, and RBAC.

These discussions will be underlined by examples of attack paths that have been found in real-world environments, discussing how it was possible to exploit misconfigurations to escalate privileges with the end goal of compromising the cluster and breaking out into the broader environment.

YouTube: https://www.youtube.com/watch?v=gwBG_oKDINQ

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

Return to Index - Add to  - ics [Calendar](#) file

Title: ATTPwn: Adversarial Emulation and Offensive Techniques Collaborative Project

When: Friday, Aug 7, 21:45 - 22:45 PDT

Where: Red Team Vlg

Speakers: Fran Ramirez, Pablo Gonzalez

SpeakerBio: Fran Ramirez

Fran Ramirez has a University degree in Computing Engineering, a Certificate of higher education in Industrial and Digital Electronics, and a Master's degree in Cybersecurity. He has experience working as an IT Senior System Engineer in the USA and Canada, consolidating IT technologies and datacenters. He began working as a Security Researcher at Telefonica and ElevenPaths in 2017. Francisco has also co-written books about Docker and Machine Learning, and been a speaker at Mobile World Congress (Barcelona), Black Hat Europe Arsenal (London), Hacktivity (Hungary), LeHack (Paris) and many other conferences.

SpeakerBio: Pablo Gonzalez

Pablo Gonzalez has a University degree in Computing Engineering and Master's degree in Cybersecurity. He has presented at Black Hat Europe Arsenal (2017, 2018, 2019), BlackHat USA Arsenal 2020, EkoParty 2018, 8dot8 Chile, DragonJAR Colombia, RootedCON, LeHACK 2019, etc. He is a Microsoft MVP 2017-2020. Pablo has written several computer security books, including Metasploit for Pentesters, Ethical Hacking, Pentesting with Kali, Metasploit hacking, Got Root and PowerShell pentesting. He is also a co-founder of flu-project and the founder of hackersClub. With more than 10 years working in cybersecurity and teaching several masters in cybersecurity in Spain, he is currently working as Project/Team Manager and Security Researcher at Telefonica (Ideas Locas department).

Description:

ATTPwn is a computer security open source tool designed to emulate adversaries. The tool aims to bring emulation of a real threat into closer contact with implementations based on the techniques and tactics from the MITRE ATT&CK framework. The goal is to simulate how a threat works in an intrusion scenario, where the threat has been successfully deployed. It is focused on Microsoft Windows systems through the use of the Powershell command line. This enables the different techniques based on MITRE ATT&CK to be applied. ATTPwn is designed to allow the emulation of adversaries as for a Red Team exercise and to verify the effectiveness and efficiency of the organization's controls in the face of a real threat. Furthermore, ATTPwn provides the possibility of knowledge transfer between users. This knowledge is exchanged through implementation of ATT&CK techniques. This new user-generated knowledge can be shared with the community through a special feature within ATTPwn. The collaborative part of ATTPwn enhances the know-how that every users can bring to the community in the shape of offensive techniques, which are always being mapped with ATT&CK.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Automating Threat Hunting on the Dark Web and other nitty-gritty things

When: Saturday, Aug 8, 19:00 - 19:59 PDT

Where: Red Team VIg

SpeakerBio: Apurv Singh Gautam

Apurv Singh Gautam is pursuing his Master's in Cybersecurity from Georgia Tech. He commenced work in Threat Intel/Hunting 2 years ago. Throughout his professional career, he worked on hunting threats from both clear web and dark web and is also involved in performing HUMINT on the d2web. He is very passionate about giving back to the community and has already conducted several talks and seminars in local security meetups, schools, and colleges. He loves volunteering with Cybrary and Station X to help students make their way in Cybersecurity. He looks forward to the end of the day to play and stream one of the AAA games Rainbow Six Siege.

Description:

What's the hype with the dark web? Why are security researchers focusing more on the dark web? How to perform threat hunting on the dark web? If you are curious about the answers to these questions, then this talk is for you. Dark web hosts several sites where criminals buy, sell, and trade goods and services like drugs, weapons, exploits, etc. Hunting on the dark web can help identify, profile, and mitigate any organization risks if done timely and appropriately. This is why threat intelligence obtained from the dark web can be crucial for any organization. In this presentation, you will learn why threat hunting on the dark web is necessary, different methodologies to perform hunting, the process after hunting, and how hunted data is analyzed. The main focus of this talk will be automating the threat hunting on the dark web. You will also get to know what operational security (OpSec) is and why it is essential while performing hunting on the dark web and how you can employ it in your daily life.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

Return to Index - Add to  - ics [Calendar](#) file

CHV - Friday - 15:00-15:50 PDT

Title: Automotive Ethernet for the rest of us

When: Friday, Aug 7, 15:00 - 15:50 PDT

Where: Car Hacking VIg 101

SpeakerBio:Infenet

Lifelong hacker and hacker of all the things. Founder of Enterprise Offensive Security, creator of security tools for DevOps Engineers such as auto-remediation using AWS Lambda and CIS Compliance Scanning Tools, SSO implementations on the Service Provider and Identity Provider side(s). Simulated Advanced Persistent Threat Actor. Started DEFCON group in Detroit DC313 and Director of #misc Detroit.

Description:

Discover the latest in Automotive Ethernet adoption, learn who is using Automotive Ethernet and why are they using Automotive Ethernet.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

CHV - Saturday - 15:00-15:50 PDT

Title: Automotive Ethernet for the rest of us

When: Saturday, Aug 8, 15:00 - 15:50 PDT

Where: Car Hacking VIg 101

SpeakerBio:Infenet

Lifelong hacker and hacker of all the things. Founder of Enterprise Offensive Security, creator of security tools for DevOps Engineers such as auto-remediation using AWS Lambda and CIS Compliance Scanning Tools, SSO implementations on the Service Provider and Identity Provider side(s). Simulated Advanced Persistent Threat Actor. Started DEFCON group in Detroit DC313 and Director of #misc Detroit.

Description:

Discover the latest in Automotive Ethernet adoption, learn who is using Automotive Ethernet and why are they using Automotive Ethernet.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Automotive In-Vehicle Networks

When: Friday, Aug 7, 10:00 - 10:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Kamel Ghali

Kamel Ghali is a veteran of the automotive security industry, with experience working both within the automotive industry and as an external consultant. His passion for automotive security goes beyond his work, with him volunteering as an instructor for the Society of Automotive Engineers (SAE) Cyber Auto Challenge and leading the Japanese branch of the Automotive Security Research Group (ASRG). He's a two-time finalist of the Car Hacking Village's annual DefCon CTF and active member of the CHV community. He currently works at White Motion, an automotive cybersecurity firm based in Tokyo, Japan.

Description:

Modern vehicles are home to tens of Electronic Control Units (ECUs) that each manage a different subsystem of the vehicle. With the control of the vehicle distributed across so many machines, sharing information in a robust, timely manner becomes a necessity. In-Vehicle Networks were developed to meet these communication needs, bringing functionality optimized for the automotive environment into the industry. In this CHV101 lecture, we'll explore the different In-Vehicle Network technologies used in vehicles today and each of their strengths and applications.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Automotive In-Vehicle Networks

When: Saturday, Aug 8, 10:00 - 10:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Kamel Ghali

Kamel Ghali is a veteran of the automotive security industry, with experience working both within the automotive industry and as an external consultant. His passion for automotive security goes beyond his work, with him volunteering as an instructor for the Society of Automotive Engineers (SAE) Cyber Auto Challenge and leading the Japanese branch of the Automotive Security Research Group (ASRG). He's a two-time finalist of the Car Hacking Village's annual DefCon CTF and active member of the CHV community. He currently works at White Motion, an automotive cybersecurity firm based in Tokyo, Japan.

Description:

Modern vehicles are home to tens of Electronic Control Units (ECUs) that each manage a different subsystem of the vehicle. With the control of the vehicle distributed across so many machines, sharing information in a robust, timely manner becomes a necessity. In-Vehicle Networks were developed to meet these communication needs, bringing functionality optimized for the automotive environment into the industry. In this CHV101 lecture, we'll explore the different In-Vehicle Network technologies used in vehicles today and each of their strengths and applications.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Autonomous Security Analysis and Penetration Testing (ASAP)

When: Sunday, Aug 9, 08:30 - 09:30 PDT

Where: Red Team Vlg

SpeakerBio: Ankur Chowdhary

Ankur Chowdhary is a PhD candidate at Arizona State University (ASU). His research interests include Cloud Security, Software Defined Networks, and application of Artificial Intelligence and Machine Learning in the field of cybersecurity. Ankur has over 5 years of cybersecurity industry experience. He has worked for companies like CSC Pvt. Ltd., Republic Services, Blackberry Pvt. Ltd., and Bishop Fox. Ankur has co-authored over 25 research papers and one textbook in the field of cybersecurity. Ankur co-founded cybersecurity startup CyNET LLC (2017). Ankur has been quite active in cybersecurity education. Ankur was ASU's National Cybersecurity Defense Competition (NCCDC) captain (2015-2018), and he is current team coach (2018-). He co-founded hacking club DevilSec in 2019 to teach offensive and defensive security to students at ASU.

Description:

Penetration Testing (Pentesting) involves skilled cybersecurity professionals generating a plan of attack for finding and exploiting vulnerabilities in the networks, and applications. The current procedure used in pen-testing is semi-automated at best and requires significant human effort. Moreover, the plan of attack followed by pen-testers may not yield best outcomes in terms of exploiting vulnerabilities in the provided time. Our framework, ASAP utilizes software vulnerabilities and network topology information to provide an artificial intelligence-based automated attack plan. Our framework Autonomous Security Analysis and Penetration Testing (ASAP) utilizes the reachability information between different network hosts and software vulnerabilities to generate a state transition graph known as attack graph. Each state in the attack graph represents the current privilege of the attacker. The attack graph also encodes information about the possible next state transitions in the network. In effect attack graph maps all possible exploits and privilege escalations possible in a network. This information is provided to Artificial Intelligence (AI) module. The AI module utilizes a popular framework known as Partially Observable Markov Decision Process (POMDP) to encode uncertainty over different state transitions, and reward obtained by attackers on achieving different privilege levels. The output generated by the AI module - Attack Policy provides the best course of action for a penetration tester/ red team member in the current network setup. The attack policy generated by the ASAP framework can be deployed on target enterprise networks using automated exploitation tools such as Metasploit. Based on our experimental evaluation in a cloud network setup, the attack policy generated by our framework does significantly better than human penetration testers in terms of finding and exploiting vulnerabilities in a network.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Aviation Privacy Treasure Hunt

When: Friday, Aug 7, 09:00 - 15:59 PDT

Where: Aerospace Vlg

SpeakerBio: Martin Strohmeier

Martin Strohmeier is a Junior Research Fellow of Kellogg College, University of Oxford and a Senior Scientist at the Swiss Cyber Defence Campus. The main focus of his work has been the design, implementation, and analysis of security protocols for cyber-physical systems, specifically those used in critical infrastructures such as aviation (civil and military). Using these domains as a driver for the real-world applicability of his research, his work has been published in many diverse venues, spanning wireless communications, cryptography, systems security, sensor networking, privacy, and aviation.

After his DPhil, he has been extending his interests towards areas of open-source intelligence, privacy issues in aviation and satellite environments, and most recently adversarial machine learning. Martin is also a co-founder of the aviation research network OpenSky where he is responsible for communication and research activities.

Description:

This OSINT CTF sends the participant on a wild treasure hunt across open aviation data, demonstrating the severe impact of some of the issues surrounding aviation tracking and datalink privacy. The participants will learn how the lack of security in wireless protocols affects the privacy of passengers and aircraft operators alike and how to exploit them. This treasure hunt will cover privacy leaks on datalinks and ATC communication used by corporate, government, military and commercial aircraft. We will actively engage with countermeasures and mitigations, showing which ones are helpful and which ones are not. This will include the most current industry attempts, including the FAA's Privacy ICAO Address programme and ACARS encryption measures. For this CTF, we will use a mixture of OSINT data sources available on the web, exclusive real-world datasets, and mock data based on our research over the past five years.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Azure AD Logs for the Blue Team (Intermediate)

When: Sunday, Aug 9, 15:00 - 15:45 PDT

Where: Blue Team Vlg - Workshop Track 1

SpeakerBio: Mark Morowczynski

Mark Morowczynski (@markmorow) is a Principal Program Manager on the customer success team in the Microsoft Identity division. He spends most of his time working with customers on their deployments of Azure Active Directory. Previously he was Premier Field Engineer supporting Active Directory, Active Directory Federation Services and Windows Client performance. He was also one of the founders of the AskPFEPlat blog. He's spoken at various industry events such as Black Hat 2019, Bsides, Microsoft Ignite, Microsoft Inspire, Microsoft Ready, Microsoft MVP Summits, The Cloud Identity Summit, SANs Security Summits and TechMentor. He can be frequently found on Twitter as @markmorow arguing about baseball and making sometimes funny gifs.

Twitter: [@markmorow](https://twitter.com/markmorow)

Description:

As enterprises move to cloud resources like Office365 and Azure AD it is imperative that they proactively monitor and protect against potential threats. But these vast quantities of security data are of no value if you, as a security admin, cannot make sense of it. In this session we'll explore the data that's available in Azure AD logs, how to integrate it with 3rd party SIEMs and get actionable insights from it. We'll also share the best practices on consuming Azure AD logs based on our insights from working with large enterprises.

Outline

Understanding the different types of logs in Azure AD (Sign-In, Audit, Risk, Application) what data is in each of them. (15 mins) Example Conditional Access Sign-in Logs (2 mins) Example Service Principal Log (2 mins) Understanding how to send logs to SIEMs (5 mins) Demo Configuring Azure Monitor Event Hub to send to 3rd party SIEM (2 mins) Understanding key events to look for and why (10 mins) Demo Using Azure work books and Log Analytics to look for key events (5 mins) Q and A (Remaining time)

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 10:30-10:59 PDT

Title: Baby's First 100 MLSec Words

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: AI Vlg

SpeakerBio:erickgalinkin

No BIO available

Twitter: [@erickgalinkin](https://twitter.com/erickgalinkin)

Description:No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Back to the future: Computer science and systems biology

When: Saturday, Aug 8, 01:00 - 01:59 PDT

Where: Red Team Vlg

Speakers:Dr Lorenz Adlung, Noa Novogroder

SpeakerBio:Dr Lorenz Adlung

Dr. Lorenz Adlung (@lorenzadlung) obtained his PhD from Heidelberg University in Germany. Since 2017 he's a visiting scientist at the Weizmann Institute of Science in Israel working in the field of computational biology, with strong emphasis on both, the computation and the biology. Besides his profession, his main passion is science communication, preferably through poetry and performance.

SpeakerBio:Noa Novogroder

Noa Novogroder (@noanovo) graduated from the first round of the Israeli cyber security academy and is currently a master student at the Weizmann Institute of Science in Israel. Before turning into biology, she's worked for several years at Checkpoint, an Israeli high-tech company in the field of cyber security. In her free time, she likes to swim and offer cure to obese mice.

Twitter: [@noanovo](https://twitter.com/noanovo)

Description:

Which creature implemented code injection 1.5 billion years before any computer malware did? What is the decoding algorithm being used in each of our cells to run the program written in our genes? As computer scientists, we are pushing the edge to develop disruptive technologies for the future. In fact, we can learn from an industry that has been evolving since long before humankind existed: The evolution of biological systems. With our proposal we hope to show the incredible parallels between bacteria and computer malware, the complex algorithms implemented in each of our cells, and how each plays a pivotal role in furthering the research of the other. This lecture will take the audience on an educational journey through both disciplines. This will foster interdisciplinary collaboration and inspire innovative solutions to future challenges for instance in the context of synthetic biology (i.e. creating artificial life), or personalized medicine (i.e. machine learning to treat patients). We are made up of trillions of computational devices. The cells within our body are information-processing units, with memory, storage, cooling and communication devices. Hardware for executable programs was very successfully shaped during the evolution of uncountable biological entities. We are presenting a wormhole between the two parallel universes of computer science and systems biology. A leap through space and time will allow us to connect the evolution of life with recent advances in computer science. An intimate exchange between the computational and the biological spheres is a prerequisite for future generations to work together on aspects of gene editing, robotics and artificial intelligence. As an incentive, we will perform a small quiz during our lecture with attractive prizes. It is our firm belief that we are the right team to foster discussions on life-inspired computer (r)evolution. Lorenz holds a PhD in Systems Biology and works as a freelancing author, consultant and keynote speaker besides being a visiting scientist at the Weizmann Institute of Science, Israel. Noa is a cyber-security expert with seven years of work experience in a high-profile IT company in Israel. Together we will stir an interactive debate on the subject.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bad Active Directory (BAD)

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: Packet Hacking VIg - Workshop

Speakers:Dhruv Verma,Michael Roberts,Xiang Wen Kuan

SpeakerBio:Dhruv Verma , Senior Security Consultant, NCC Group

Dhruv Verma is a Senior Security Consultant at NCC Group, an information security firm specializing in application, network, and mobile security. Dhruv has extensive experience performing infrastructure assessments with a special interest in Windows Active Directory environments and projects involving social engineering vectors. He has gotten domain admin on multiple client networks by chaining together vulnerabilities in a very unique and interesting fashion. For instance, Dhruv combined a misconfigured Jenkins server with a AWS IAM privilege escalation attack to gain Domain Admin on an enterprise network via a clone'n'pwn attack.

SpeakerBio:Michael Roberts , Senior Security Consultant, NCC Group

Michael Roberts is a Senior Security Consultant with NCC Group. Michael performs web, mobile application and network penetration tests, and has a passion for virtual reality and cooking outside of work life. Michael holds an bachelor's degree in computer and information technology from Purdue University.

SpeakerBio:Xiang Wen Kuan , Security Consultant, NCC Group

Xiang Wen Kuan is a Security Consultant at NCC Group. Kuan has conducted some infrastructure assessments and first started BAD under the supervision of Dhruv and Michael as his intern project at NCC. Kuan is as exciting as Kashi cereal and likes to eat free food at hacker events.

Description:

This is an introductory to intermediate level Windows active directory (AD) training. The training has two parts: a lecture component, where we'll cover how active directory works and the core things you need to know to attack it effectively, and a series of hands-on labs modeled after real attacks we've performed on client environments. The training will be heavily lab focused, with each student receiving their own AWS environment to play with. The labs are based off of how real modern networks look, not example test environments, and successfully completing each lab involves chaining together multiple vulnerabilities in a realistic kill chain methodology to get domain admin.

This workshop requires registration. If you are registered, please proceed to #phv-infobooth-text and you'll be given access to join.

#phv-infobooth-text: <https://discord.com/channels/708208267699945503/708242376883306526>

Return to Index - Add to  - ics [Calendar](#) file

MOV - Saturday - 13:30-14:30 PDT

Title: Badge Clinic

When: Saturday, Aug 8, 13:30 - 14:30 PDT

Where: Monero Vlg

SpeakerBio:Michael Schloh von Bennewitz

No BIO available

Description:

With the help of a close range circuit camera, Michael illustrates the circuits of several recent conference hardware devices, including prototype models. Devices in circulation and on display include: DC28 Intervillage Badge DC27 Rising Badge 35C3 Blockchain DC26/BCOS Badge HCPP19 Badge HCPP18 Badge This is not a speech presentation, rather it is an easy office hours with show and tell to invite questions and answers about low power electronic devices. Visit the Badge Clinic on any day of Defcon in the Monero Village channel.

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/70820826769945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Sunday - 13:30-14:30 PDT

Title: Badge Clinic

When: Sunday, Aug 9, 13:30 - 14:30 PDT

Where: Monero Vlg

SpeakerBio:Michael Schloh von Bennewitz

No BIO available

Description:

With the help of a close range circuit camera, Michael illustrates the circuits of several recent conference hardware devices, including prototype models. Devices in circulation and on display include: DC28 Intervillage Badge DC27 Rising Badge 35C3 Blockchain DC26/BCOS Badge HCPP19 Badge HCPP18 Badge This is not a speech presentation, rather it is an easy office hours with show and tell to invite questions and answers about low power electronic devices. Visit the Badge Clinic on any day of Defcon in the Monero Village channel.

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/70820826769945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCG - Saturday - 12:00-12:59 PDT

Title: Basic OSINT: Mining Personal Data

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: DEF CON Groups

Description:

Presentation by DC574 (Indiana, USA)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Be Like Water: What Bruce Lee Can Teach Us About AppSec

When: Saturday, Aug 8, 09:00 - 09:59 PDT

Where: AppSec Vlg

SpeakerBio: Fredrick "Flee" Lee

No BIO available

Twitter: [@fredrickl](#)

Description:

Every few years, security “thought leaders” tell us what is the one, proper way to practice application security. I’m just as guilty of this as anyone else in the “industry”. But, it turns out there isn’t just one true style of effective AppSec. This talk walks through my path of letting go of dogma, finding my style, and returning back to always being a student of the game. “Absorb what is useful, reject what is useless, add what is essentially your own.”

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

Return to Index - Add to  - ics [Calendar](#) file

CNE - Friday - 09:00-17:59 PDT

Title: Be the Match - registration drive

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Be the Match registration drive is returning once again! Swing by and check out one of the coolest biohacks out there, and how you could be the next person to save a life through cellular therapy.

Discord: <https://discord.com/channels/708208267699945503/711643405004046457>

Web: <https://bethematch.org>

Return to Index - Add to  - ics [Calendar](#) file

Title: Be the Match - registration drive

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Be the Match registration drive is returning once again! Swing by and check out one of the coolest biohacks out there, and how you could be the next person to save a life through cellular therapy.

Discord: <https://discord.com/channels/708208267699945503/711643405004046457>

Web: <https://bethematch.org>

Return to Index - Add to  - ics [Calendar](#) file

Title: Be the Match - registration drive

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Be the Match registration drive is returning once again! Swing by and check out one of the coolest biohacks out there, and how you could be the next person to save a life through cellular therapy.

Discord: <https://discord.com/channels/708208267699945503/711643405004046457>

Web: <https://bethematch.org>

Return to Index - Add to  - ics [Calendar](#) file

Title: Before J1939: A J1708/J1587 Protocol Decoder

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: Car Hacking VIg 002

Speakers: Thomas Hayes, Dan Salloum

SpeakerBio: Thomas Hayes

Thomas Hayes is a Hardware Engineer at Bendix Commercial Vehicle Systems in Elyria, OH and a member of the SAE J1939 committees. In his current role, he manages the hardware process for braking and other heavy vehicle systems from brainstorming with napkin drawings to the creation of full PCBs to product testing and manufacturing. Prior to Bendix Thomas held design and leadership roles in a number of venture backed startups and worked in simulation technology for the aviation industry. In his spare time, Thomas enjoys rebuilding vintage motorcycles and teaching kids how to solder without burning their fingers off: success rate unknown.

SpeakerBio: Dan Salloum

Daniel Salloum is a Reverse Engineer by title and curious at heart. He is currently employed by Assured Information Security where he spends his days doing security evaluations and creating tools that help. His background as both a system administrator and programmer help him to navigate system innards. If it must be done more than twice, he'll script it. If it can be recreated in a few hours, it probably will be. Daniel has recently been accepted into the world of ham radio, and may be heard on the airwaves at some point. This is his first conference and expects it won't be the last.

Description:

Medium and heavy duty equipment communicate over vehicle networks using a number of protocols and busses. While researching the interaction between tractors and semi-trailers, we identified the presence of two legacy protocols, J1708 (physical layer), and J1587 (transport layer). The current mechanisms to capture and decode this data do not promote cost efficient data DISCOVERY, but as a team, we have developed techniques that will allow us to use existing diagnostic hardware to capture and decode J1587, and J1708, messages from the vehicle bus.

pretty_1587, our software application, has been designed to process input streams and convert SAE J1708 and J1587 messages to a convenient format that a user can read or pass to another software application. Our open source python code has been designed to be versatile and to work with the output of existing diagnostic tools and can consume data over network sockets, from files, or from stdin, allowing most hardware solutions that interface directly with the serial bus will be able to pass data to pretty_1587 to decode the data contained in the J1587 messages.

#chv-track002-text: <https://discord.com/channels/708208267699945503/739564953014632579>

YouTube: <https://www.youtube.com/watch?v=5DYhXbWkWoA&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack002>

Return to Index - Add to  - ics [Calendar](#) file

Title: Beyond Root: Custom Firmware for Embedded Mobile Chipsets

When: Sunday, Aug 9, 14:30 - 14:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Christopher Wade , Security Consultant at Pen Test Partners

Chris is a seasoned security researcher and consultant. His main focuses are in reverse engineering hardware, fingerprinting USB vulnerabilities and playing with Software Defined Radios, with his key strength lying in firmware analysis, which he utilizes as part of the hardware testing team at Pen Test Partners.

Description:

Rooting a smartphone is often considered the ultimate method to allow a user to take complete control of their device. Despite this, many smartphones contain hardware which is closed off to any modification. This talk aims to show how this hardware can be reverse engineered in order to bypass its protections and further expand its functionality.

Using proprietary NFC Controllers as an example, we will cover analysis of the protocols used by the chips, how the firmware protections could be broken, and how custom firmware could be developed and deployed to the phone with no hardware modifications. This will include methodologies for analyzing weaknesses in firmware update protocols, leveraging the Unicorn CPU Emulator to bypass debugging restrictions, and techniques for reverse engineering the hardware capabilities of an unknown chip in order to implement custom features. This will end with demonstration of a smartphone with passive NFC sniffing capabilities and expanded tag emulation functionality.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bio-Hacking - Hospital Under Siege

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Adversaries have gained a foothold in your local hospital and are increasing their control over clinical systems and medical devices. Soon they make it clear they're not after patient records or financial information, but are out to disrupt care delivery and put patients lives at risk. Your team received an urgent request to use your blue, red, and purple team skills to defend against the escalating attacks, attempt to unmask the adversary, and - above all - protect patient lives.

Hospital Under Siege is a scenario-driven Capture the Flag contest run by the Biohacking Village, pitting teams of participants against adversaries and against a clock, to protect human life and public safety. Participants will compete against each other on both real and simulated medical devices, in the fully immersive Biohacking Village: Device Lab, laid out as a working hospital. Teams of any size are welcome, as are players from all backgrounds and skill levels. 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 exotic protocols like DICOM, HL7 and FHIR.

Forum: <https://forum.defcon.org/node/232894>

Discord: <https://discord.com/channels/708208267699945503/711643365120278540>

Twitter: https://twitter.com/DC_BHV

Web: <https://www.villageb.io/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Bio-Hacking - Hospital Under Siege

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Adversaries have gained a foothold in your local hospital and are increasing their control over clinical systems and medical devices. Soon they make it clear they're not after patient records or financial information, but are out to disrupt care delivery and put patients lives at risk. Your team received an urgent request to use your blue, red, and purple team skills to defend against the escalating attacks, attempt to unmask the adversary, and - above all - protect patient lives.

Hospital Under Siege is a scenario-driven Capture the Flag contest run by the Biohacking Village, pitting teams of participants against adversaries and against a clock, to protect human life and public safety. Participants will compete against each other on both real and simulated medical devices, in the fully immersive Biohacking Village: Device Lab, laid out as a working hospital. Teams of any size are welcome, as are players from all backgrounds and skill levels. 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 exotic protocols like DICOM, HL7 and FHIR.

Forum: <https://forum.defcon.org/node/232894>

Discord: <https://discord.com/channels/708208267699945503/711643365120278540>

Twitter: https://twitter.com/DC_BHV

Web: <https://www.villageb.io/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Bio-Hacking - Hospital Under Siege

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Adversaries have gained a foothold in your local hospital and are increasing their control over clinical systems and medical devices. Soon they make it clear they're not after patient records or financial information, but are out to disrupt care delivery and put patients lives at risk. Your team received an urgent request to use your blue, red, and purple team skills to defend against the escalating attacks, attempt to unmask the adversary, and - above all - protect patient lives.

Hospital Under Siege is a scenario-driven Capture the Flag contest run by the Biohacking Village, pitting teams of participants against adversaries and against a clock, to protect human life and public safety. Participants will compete against each other on both real and simulated medical devices, in the fully immersive Biohacking Village: Device Lab, laid out as a working hospital. Teams of any size are welcome, as are players from all backgrounds and skill levels. 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 exotic protocols like DICOM, HL7 and FHIR.

Forum: <https://forum.defcon.org/node/232894>

Discord: <https://discord.com/channels/708208267699945503/711643365120278540>

Twitter: https://twitter.com/DC_BHV

Web: <https://www.villageb.io/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Blackmail, Extortion and the Ethics of Disclosure

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: Ethics VIg

SpeakerBio:Michael Antonino

No BIO available

Description:

This will be a live talk.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar file](#)

BCV - Saturday - 13:00-13:30 PDT

Title: Blockchain for Cyber Defense: Will it be as good as you think?

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: Blockchain VIg

Speakers:Seungjoo,Suhyeon Lee

SpeakerBio:Seungjoo

No BIO available

SpeakerBio:Suhyeon Lee

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Blue Team Village & Red Team Village Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Blue Team Vlg - Talks Track 1

Speakers: Joseph Mlodzianowski (cedoXx), Adam Mashinchi, Plug, Dani, Jorge Orchilles, David J. Bianco

SpeakerBio: Joseph Mlodzianowski (cedoXx)

No BIO available

Twitter: [@cedoxX](#)

SpeakerBio: Adam Mashinchi

Adam Mashinchi is SCYTHE's VP of Product Management where he leads the project management, design, and quality assurance departments for SCYTHE's product portfolio. Before SCYTHE, Adam defined and managed the development of enterprise security and privacy solutions with an emphasis on usable encryption at a global scale and led numerous technical integration projects with a variety of partners and services.

Twitter: [@adam_mashinchi](#)

SpeakerBio: Plug

No BIO available

Twitter: [@plugxor](#)

SpeakerBio: Dani

No BIO available

Twitter: [@_ChezDaniela](#)

SpeakerBio: Jorge Orchilles

No BIO available

Twitter: [@jorgeorchilles](#)

SpeakerBio: David J. Bianco

David is a defensive security researcher specializing in incident detection & response. His major focus areas are threat hunting and the strategic consumption of Cyber Threat Intelligence. He's currently a Principal Engineer, Cybersecurity at a major US retailer.

David is probably most well known as the originator of the Pyramid of Pain and the Hunting Maturity Model. You can follow him online via Twitter [@DavidJBianco](#) or subscribe to his blog, Enterprise Detection & Response.

Twitter: [@DavidJBianco](#)

Description: No Description available

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bluetooth Security in Automotive

When: Friday, Aug 7, 14:00 - 14:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Kamel Ghali

Kamel Ghali is a veteran of the automotive security industry, with experience working both within the automotive industry and as an external consultant. His passion for automotive security goes beyond his work, with him volunteering as an instructor for the Society of Automotive Engineers (SAE) Cyber Auto Challenge and leading the Japanese branch of the Automotive Security Research Group (ASRG). He's a two-time finalist of the Car Hacking Village's annual DefCon CTF and active member of the CHV community. He currently works at White Motion, an automotive cybersecurity firm based in Tokyo, Japan.

Description:

Bluetooth is a short-range cable replacement technology that is found in millions of IoT devices around the world. Due to its ubiquity and breadth of functionality, it's been seen in vehicles as early as the late 2000s. While commonly used for phonebook access, hands-free phone usage, and media control, Bluetooth is nonetheless an important vector to consider when analyzing a vehicle's security case. In this CHV101 lecture, we'll explore Bluetooth as a technology and its relevance to automotive cybersecurity.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bluetooth Security in Automotive

When: Saturday, Aug 8, 14:00 - 14:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Kamel Ghali

Kamel Ghali is a veteran of the automotive security industry, with experience working both within the automotive industry and as an external consultant. His passion for automotive security goes beyond his work, with him volunteering as an instructor for the Society of Automotive Engineers (SAE) Cyber Auto Challenge and leading the Japanese branch of the Automotive Security Research Group (ASRG). He's a two-time finalist of the Car Hacking Village's annual DefCon CTF and active member of the CHV community. He currently works at White Motion, an automotive cybersecurity firm based in Tokyo, Japan.

Description:

Bluetooth is a short-range cable replacement technology that is found in millions of IoT devices around the world. Due to its ubiquity and breadth of functionality, it's been seen in vehicles as early as the late 2000s. While commonly used for phonebook access, hands-free phone usage, and media control, Bluetooth is nonetheless an important vector to consider when analyzing a vehicle's security case. In this CHV101 lecture, we'll explore Bluetooth as a technology and its relevance to automotive cybersecurity.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bobby Pins, More Effective Than Lockpicks?

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: Lockpick Vlg

SpeakerBio:John the Greek

No BIO available

Description:

When should you not have picks in your pocket? Answer, never... but

This course will present to the novice and the less prepared suggestions for improvising lockpicks when the proper tools are not on hand as well as techniques of bypass that are more effective than trying to pick a lock especially when you don't have the proper tools on hand. This class is ideal for our current situation! Those interested should look around their locations for the following:

- Bobby pins
- Paper clips (big ones)
- Pocket clips from ink pens (Pilot rollerball) Old Wind Shield Wipers
- Spark Plug Gappers
- Bra Underwire

... and my favorite
Street cleaner bristles

The course will take approximately and hour

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Breakdown Of The FAA's Privacy ICAO Address Program

When: Sunday, Aug 9, 13:30 - 13:59 PDT

Where: Aerospace Vlg

SpeakerBio: Gui Michel

Gui is a Master student in the joint degree in Cybersecurity at EPFL and ETH Zürich. His research interests lie in distributed systems, computer security and privacy.

Description:

The FAA launched the Privacy ICAO Address (PIA) program in January 2020 to address privacy concerns in General Aviation in the United States. This talk will present an analysis on the privacy performance of this program in its current state and our predictions for the future. We will demonstrate that it is possible to identify aircraft despite being enrolled in the program, using ADS-B data from crowdsourced networks. The privacy loss of participating aircraft over time is quantified through a purpose-built privacy simulator, showing that tracking is possible, even with a much greater participation in the program in the future. To address these issues, we will present two solutions that could significantly improve the privacy of the PIA program going forward.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Breaking the Attack Chain

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: Red Team VIg

Speakers: Corey Ham, Matt Eidelberg

SpeakerBio: Corey Ham

Corey Ham & Matt Eidelberg are principal consultants/leaders within Optiv's advanced services sub-team. Together they have 13 years combined experience delivering offensive security engagements for clients, along with personal tool development and research.

SpeakerBio: Matt Eidelberg

Corey Ham & Matt Eidelberg are principal consultants/leaders within Optiv's advanced services sub-team. Together they have 13 years combined experience delivering offensive security engagements for clients, along with personal tool development and research. Matthew has presented at multiple conferences across North America.

Description:

Despite the rising tide of security maturity, targeted attack chains are often successful due to systemic weaknesses in how modern IT administrators and blue teams operate. This talk gives the attacker's perspective on how common attack chains can be stopped before they spiral out of control. This talk is fueled by two red team operators field experience in attacking modern enterprise environments. It will cover various tactics and techniques that are used with high success during red team engagements, as well as specific countermeasures that would hamper the success of the described attack chains. The speakers will cover a hypothetical red team style engagement, starting from a limited-knowledge basis on the Internet, moving to an internal foothold, leading to data compromise. This talk will focus on technical details at an executive level, and will be performed in a "debrief" style with no technical specifics or demos.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AEV - Friday - 12:00-17:59 PDT

Title: Bricks in the Air

When: Friday, Aug 7, 12:00 - 17:59 PDT

Where: Aerospace VIg Workshop

Description:

A huge hit at Def Con 27, we've partnered with the Defense Digital Service to bring back Bricks-In-The-Air for #DEFCON28SafeMode. Whether you're a noob or a pro, this is your chance to attempt sending messages to mock LEGO aircraft over I2C to learn and experiment with direct injection attacks on a data bus.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bricks in the Air

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

A huge hit at Def Con 27, we've partnered with the Defense Digital Service to bring back Bricks-In-The-Air for #DEFCON28SafeMode. Whether you're a noob or a pro, this is your chance to attempt sending messages to mock LEGO aircraft over I2C to learn and experiment with direct injection attacks on a data bus.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bricks in the Air

When: Sunday, Aug 9, 09:00 - 13:59 PDT

Where: Aerospace VIg Workshop

Description:

A huge hit at Def Con 27, we've partnered with the Defense Digital Service to bring back Bricks-In-The-Air for #DEFCON28SafeMode. Whether you're a noob or a pro, this is your chance to attempt sending messages to mock LEGO aircraft over I2C to learn and experiment with direct injection attacks on a data bus.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HTS - Friday - 12:00-12:59 PDT

Title: Build a Raspberry AIS

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: Hack the Sea Vlg

SpeakerBio:Dr. Gary Kessler

No BIO available

Description:No Description available

Hack the Sea Village activities will be streamed to Twitch.

Twitch: <https://twitch.tv/hackthesea>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Sunday - 11:00-11:59 PDT

Title: Building a Microcontroller Bitcoin Address Generator

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: Blockchain Vlg

Speakers:chaintuts,Josh McIntyre

SpeakerBio:chaintuts

No BIO available

SpeakerBio:Josh McIntyre

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

ICS - Saturday - 14:15-15:15 PDT

Title: Building a Physical Testbed for Blackstart Restoration under Cyber Fire

When: Saturday, Aug 8, 14:15 - 15:15 PDT

Where: ICS Vlg

SpeakerBio: Tim Yardley

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Building BLUESPAWN: An Open-Source, Active Defense & EDR Software (Intermediate)

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: Blue Team Vlg - Talks Track 1

Speakers: Jake Smith, Jack McDowell

SpeakerBio: Jake Smith

Jake is recent graduate of the University of Virginia where he studied Computer Science and Cybersecurity. During his time in school, he was a Rodman Scholar and served as President of the Computer and Network Security (CNS) Club at UVA. In addition, he co-started UVA's Cyber Defense and Offense Teams to compete in the Collegiate Cyber Defense Competition (CCDC) and Collegiate Penetration Testing Competition (CPTC). Outside of school, Jake co-founded MetaCTF, a cybersecurity training company, which has run CTF events across the United States and beyond.

Twitter: [@jtsmith282](https://twitter.com/jtsmith282)

SpeakerBio: Jack McDowell

No BIO available

Description:

Our team has developed BLUESPAWN, a fully open-source, active defense and EDR tool for Windows. While there are ample offensive oriented tools publicly available, there is very little on the defensive side. We aim to use this project to demonstrate how modern-day security solutions work by building our own from the ground up. In addition, we integrate a number of popular community libraries and tools such as MITRE ATT&CK, DoD STIGs, YARA, and PE-Sieve with one goal: to enable any security analyst to quickly detect, identify, and eliminate malicious activity on a system.

In today's world, computers running Microsoft's Windows operating system remain a top target for threat actors given its popularity. While there are a number of commercial defensive cybersecurity tools and multi-purpose system analysis programs such as SysInternals, this software is often closed-source, operates in a black-box manner, or requires a payment to obtain. These characteristics impose costs for both attackers and defenders. In particular, while the restrictions prevent attackers from knowing exactly what these tools detect, defenders often end up not having a good understanding of how their tools work or exactly what malicious activity they can identify.

Building on prior work and other open-source software, our team decided to create BLUESPAWN. This open-source program is an active defense and endpoint detection & response (EDR) tool designed to quickly prevent, detect, and eliminate malicious activity on a Windows system. In addition, BLUESPAWN is centered around the MITRE ATT&CK Framework and the Department of Defense's published STIGs. We have also integrated popular malware analysis libraries such as VirusTotal's YARA to increase the tool's effectiveness and accessibility. Currently, our team is developing the alpha version of the client which can already detect real-world malware. In the future, we will continue to build out the client and eventually integrate both a server component for controlling clients and a cloud component to deliver enhanced detection capabilities.

Github: <https://github.com/ION28/BLUESPAWN>

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Building Connections Across The Aviation Ecosystem

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Aerospace Vlg

Speakers:Katie Noble,Al Burke,Jeff Troy,Jen Ellis,John Craig,Randy Talley (CISA),Sidd Gejji

SpeakerBio:Katie Noble , Intel Corp

Katie currently serves as a Director of PSIRT and Bug Bounty at Intel Corp. Where she leads the cyber security vulnerability Bug Bounty program, researcher outreach, and strategic planning efforts. Previous to this position, Katie served as the Section Chief of the Vulnerability Management and Coordination at the Department of Homeland Security, Cyber and Infrastructure Security Agency (CISA) where she led DHS' primary operations arm for coordinating the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems, enterprise, hardware and software. Katies team is credited by the Secretary of Homeland Security with the coordination and public disclosure of over 20,000 cyber security vulnerabilities within a two year period. Katie is a highly accomplished manager with over 14 years of U.S. Government experience, both in the Intelligence Community and Cyber Security Program Management. She has operated at all levels from individual contributor as an Intelligence Analyst for the National Intelligence Community to Senior Policy Advisor for White House led National Security Council (NSC) Cyber programs. Her work has directly impacted the decision making of the NSC, Defense Information Systems Agency, Office of the Director of National Intelligence, Department of Defense, Federal Communications Commission, Central Intelligence Agency, U.S. Coast Guard, U.K.Ministry of Defense, Canadian Government agencies, and Australian Cabinet Ministry.

SpeakerBio:Al Burke , Associate Deputy Director, Air Force Cyberspace Operations and Warfighter Communications
Mr. Alan W. Burke is the Associate Deputy Director, Air Force Cyberspace Operations and Warfighter Communications and the DOD Chair for the interagency Aviation Cyber Initiative Task Force. Most recently he was a Distinguished Graduate of the College of Information and Cyberspace, National Defense University. He has 36-years of combined active military and government service in the U.S. Air Force and Department of Defense. Previously, he was Chief of the Integrated Air and Missile Defense (IAMD) Division, U.S. Air Forces in Europe-Africa responsible for integrating joint and coalition air, space and missile defense capabilities in support of the Joint Force Air Component Commander and implementation of Presidential policy for missile defense in Europe. On active duty, Colonel Burke was the Director, Operations Support Group and Deputy Director, Warfighter Support Center, Missile Defense Agency (MDA) that delivered global support for Ballistic Missile Defense operations and led the initial Missile Defense Agency Ballistic Missile Defense system deployments in Israel. His active duty service includes operational, staff and command experience in nuclear missile operations, space surveillance, space control, missile warning, national-level command and control, air and missile defense, military training and education, and Research, Development, Test and Evaluation.

SpeakerBio:Jeff Troy , President, CEO, Aviation ISAC

Over the past three years, Jeff developed the A-ISAC comprehensive strategy, led the team's expansion of the Aviation ISACs services, and tripled membership. He established relationships with global regulators, industry associations, and private sector companies to drive cyber risk reduction across the aviation eco-system. Concurrently, Jeff employed by General Electric and is on the Board of Directors, National Defense ISAC. ND-ISAC provides cutting edge cyber security training, intelligence development and a trusted information sharing environment for US cleared defense contractors. Jeff spent 25 years as a Special Agent of the FBI. He retired as the Deputy Assistant Director for Cyber National Security and Cyber Criminal Investigations.

SpeakerBio:Jen Ellis , Rapid7

Jen Ellis is the vice president of community and public affairs at Rapid7 and her primary focus is on advancing cybersecurity for all by building productive collaboration between those in the security community and those operating outside it. She works extensively with security researchers, technology providers and operators, and various government entities to help them understand and address cybersecurity challenges. She believes effective collaboration is our only path forward to reducing cybercrime and protecting consumers and businesses. Jen is a nonresident fellow of the Atlantic Council, sits on the boards of the Center for Cybersecurity Policy and Law, I Am The Cavalry, and the Aerospace Village, and is a member of the board of

advisors for the CyberPeace Institute. She has testified before U.S. Congress and spoken at numerous security or business conferences.

SpeakerBio:John Craig , Boeing

John Craig is currently the Chief Engineer of Cabin, Network and Security Systems and Product Security Officer for Boeing Commercial Airplanes. In this role, he is responsible for cabin systems, connectivity, onboard networks, cyber security, and airborne software design and implementation. In addition, he is the chairman of the board of the Aviation Information Sharing and Analysis Center, formed to encourage sharing of cyber threat information within the aviation industry. He is on the policy board and program management committee of RTCA to provide input for policy and programs for the aviation. In his 34 years of aviation experience, he has held roles in Electrical Subsystems, Engine Systems, Avionics, Cabin Systems, Onboard Networks, and Connectivity Systems. He is experienced in large scale systems development, software developmental programs and, as a previous FAA Designated Engineering Representative, knowledge of airplane certification programs.

SpeakerBio:Randy Talley (CISA)

Mr. Talley is a Senior Advisor assigned to the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) located in Arlington, VA. He uses his aviation expertise and operational Homeland Security background to provide aviation-specific advice to CISA leadership. In his primary role, Mr. Talley serves as the DHS Lead for the Aviation Cyber Initiative (ACI), a Tri-Chaired Task Force assigned to collaborate across the Federal Government, aviation industry and the research community to reduce risks and improve resilience within the Nation's Aviation Ecosystem.

SpeakerBio:Sidd Gejji , FAA

Siddharth (Sidd) Gejji is a Manager in the Federal Aviation Administration (FAA) Office of Information Security and Privacy, within the FAA Office of Information and Technology. Mr. Gejji leads the Aviation Ecosystem Stakeholder Engagement Branch, which is a team of experts responsible for conducting cybersecurity stakeholder engagements throughout the Aviation Ecosystem, including in the Airlines, Airports, Aviation Management, and Aircraft areas. Mr. Gejji serves as a Tri-Chair for the U.S. Aviation Cyber Initiative (ACI). The ACI is a US Government task force with Tri-Chairs from Department of Homeland Security (DHS), Department of Defense (DoD), and FAA. Mr. Gejji and his team support this important interagency mission to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation's Aviation Ecosystem. Prior to his current engagement, Sidd spent 12 years in various roles at the FAA, most notably in the FAA Office of Policy where he served as an Acting Manager of the Systems and Policy Analysis Group. He also spent a year on detail to the U.S. Senate Commerce, Science, and Transportation Committee.

Description:

Across the Aviation Ecosystem, there is an increased effort to collaborate and coordinate to protect Information Technology (IT) and Operational Technology (OT) systems at airports, airlines, aviation management, and manufacturers and vendors via the supply chain. This diverse panel will share their insights and current activities between government, industry, and the security research community. Learn how you can participate in and ensure the safety and security of the Aviation Ecosystem.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Building Teams in the New Normal

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: Career Hacking Vlg

SpeakerBio: Mike Murray

No BIO available

Description:

2020 has created massive change across our industry, both from the perspective of COVID-19 as well as the social movements that have changed the way we view ourselves. Nowhere has this affected the industry more than the experience by which we onboard employees - as an example, before 2020, even most remote employees had in person interviews in the process. In short, the "new normal" that is evolving requires us to hire and interview differently. From where and how we find (especially diverse) candidates, our interview processes and the way we onboard employees in to our culture, everything requires a thoughtful new approach. In this talk, Mike will talk about everything he has learned and how he has modified his own processes to promote diversity, find the best people to join the team, and brought them aboard as part of the culture.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Burnout is real

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: Recon Vlg

SpeakerBio: Chloé Messdaghi

Chloé Messdaghi is the VP of Strategy at Point3 Security. She is a security researcher advocate who strongly believes that information security is a humanitarian issue. Besides her passion to keep people safe and empowered online & offline, she is driven to fight for hacker rights. She is the founder of WomenHackerz & the President and cofounder of Women of Security (WoSEC), podcaster for ITSP Magazine's The Uncommon Journey, and runs the Hacker Book Club.

Description:

Mental health is an ongoing issue within infosec before and during COVID-19. There's a fine balance between hacking and personal life. Majority of the time, they cross over. This talk shares an overview of the warning signs, symptoms, and practices to prevent burnout and how to deal with burnout to keep balanced.

Recon Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/c/ReconVillage>

#rv-talks-text: <https://discord.com/channels/708208267699945503/737048009732522014>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CRV - Friday - 11:00-11:59 PDT

Title: But I Still Need A Job!

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Career Hacking Vlg

SpeakerBio: Kirsten Renner

No BIO available

Description:

As if finding your next gig wasn't already a challenge, now we have to do it in the midst of a pandemic. Let's talk about the new hurdles, how to get around them and the classic fundamentals like searching, networking, and negotiating

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bypassing Biometric Systems with 3D Printing and Enhanced Grease Attacks

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Yamila Levalle , Researcher at Dreamlab Technologies

Yamila Vanesa Levalle is an Information Systems Engineer, Security Researcher and Offensive Security Professional with more than 15 years of experience in the InfoSec area.

Yamila currently works as Security Researcher and Consultant at Dreamlab Technologies where she specializes in offensive techniques, conducts researches, gives trainings and write papers and blog posts. She is an international security conferences speaker and has presented her researches at important events such as BlackHat Arsenal Vegas, PHDays Moscow, Northsec Montreal, AusCERT Australia, 8.8 Security Conference Vegas, SCSD Fribourg, Ekoparty Ekolabs, OWASP Latam Tour and others. She has taught ethical hacking courses for women, CTF courses for beginners and several information security trainings.

Description:

Due to the well-known vulnerabilities in traditional authentication methods through users, passwords and tokens; biometric systems began to be widely implemented in millions of devices with the aim of having a more practical authentication system for users and -supposedly- more robust in terms of security.

Security researchers were not far behind and started to analyze the security of these biometric controls. In recent years, different techniques have been presented to bypass the authentication of, for example, the smartphones that began to implement these systems.

What is new in this talk? avoiding focusing on a particular device, we have gone deeper studying the operation of the sensors implemented in different biometric systems (Optical, Capacitive, Ultrasonic, Facial, etc.) and consequently, we discovered new techniques to bypass them. Through this talk, we will show how to fool biometric sensors by the enhanced grease attacks and, even better, the techniques to succeed at bypassing these controls using 3D printing.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

Return to Index - Add to  - ics [Calendar](#) file

Title: Bypassing in Mobile Network From Red-Team Points of View

When: Saturday, Aug 8, 20:15 - 21:15 PDT

Where: Red Team Vlg

SpeakerBio: Ali Abdollahi

Ali Abdollahi is a cyber security expert with over 8 years of experience working in a variety of security fields. Ali is a full-time consultant helping clients with product security testing, reverse engineering, penetration testing, exploit developing, red-teaming, secure coding, and more, giving him ample opportunity to use his skills in a diversity of ways. In addition, He is instructor, author and board of review at Hakin9 company. Ali is a self-confessed bug hunter, publisher of many vulnerabilities and CVEs. Ali is a regular speaker and trainer at industry conferences.

Twitter: [@AliAbdollahi2](https://twitter.com/AliAbdollahi2)

Description:

This talk focus on reviewing implementation of new security features in mobile networks as well as detecting techniques and bypassing methods from red team perspective . The scope of the illustration include both radio (SDR) and signalling core network attacks. - The outline of the presentation // max 500 words One of the most complicated network is mobile telecom network. There are some segments include signalling, charging, packet data, Radio etc. Still there are many security holes that allow attackers to compromise the network and however telecom companies enable security mechanisms and put some security devices. In this talk, I will cover common high-tech security solutions used by telecom operators and and all ways to detect and after that bypass it as well as security recommendations to prevent theses activities. In this talk I will start the presentation with recent telecom abuse and related hacking news in 2019. In the next section I will cover common mobile network vulnerabilities and architecture. After that illustrate security of radio access network (RAN) and bypassing scenarios and techniques: 1. Mobile Phone Registration (IMEI policies) Bypass 2. Bypassing Unrevealed Ciphering Algorithms 3. 5G, LTE/LTE Advanced Bypass

The next part of the talk will be assign to Circuit Switch network (Signaling) and the technical bypass techniques are as below:

1. Home Routing Detection
2. Bypassing Home Routing
3. Signalling Firewall Detection
4. Bypassing Signalling Firewall

And at the final section I will explain security solutions to defend against these malicious techniques.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Bytes In Disguise

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: DEF CON Q&A Twitch

Speakers:Jesse Michael,Mickey Shkatov

SpeakerBio:Jesse Michael

Jesse MichaelJesse Michael is an experienced security researcher focused on vulnerability detection and mitigation who has worked at all layers of modern computing environments from exploiting worldwide corporate network infrastructure down to hunting vulnerabilities inside processors at the hardware design level. His primary areas of expertise include reverse engineering embedded firmware and exploit development. He has also presented research at DEF CON, Black Hat, PacSec, Hackito Ergo Sum, Ekoparty, and BSides Portland.

Twitter: [@JesseMichael](#)

SpeakerBio:Mickey Shkatov

Mickey has been doing security research for almost a decade, one of specialties is simplifying complex concepts and finding security flaws in unlikely places. He has seen some crazy things and lived to tell about them at security conferences all over the world, his past talks range from web pentesting to black badges and from hacking cars to BIOS firmware.

Twitter: [@HackingThings](#)

Description:

Non-Volatile Memory. EVERY computer has it, from the chip that stores your BIOS to the controller that runs your laptop trackpad and even your new fancy USB-C monitor. These small nooks of storage can be (ab)used by anyone to store data or code without causing any side effects and none would be the wiser. We will show you more than one example of how this is possible and walk through everything you need to know to do it, too. In this talk, we will describe how to hide persistence in these obscure memory chips using simple tools that we are releasing as open source. We will show multiple ways to accomplish this without detection. On the defensive front, we'll discuss what can be done to detect and lock down systems.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cal Poly Workshop - Simulated Satellite Communications on Raspberry Pi

When: Friday, Aug 7, 09:00 - 15:59 PDT

Where: Aerospace Vlg Workshop

Description:

Users will need to purchase own equipment before the workshop/challenge is run. (users will attempt to see simulated altitude, battery level, telemetry data from the mock satellite. It will be awesome because, we will expose participants new to the convergence of space and cybersecurity a crawl/beginner experience to gain their interest. It's designed as a workshop. The Convergence of Space & Cybersecurity Innovation.

The goal of this workshop would be to construct a “CubeSat Simulator Lite

<https://github.com/alanbjohnston/CubeSatSim/wiki> specifically

<https://github.com/alanbjohnston/CubeSatSim/wiki/CubeSat-Simulator-Lite>.

We would run through the installation of the software via a screensharing method. We'd show participants how to setup a Raspberry Pi, set up the device, install the necessary packages, attach a necessary antenna, and view the transmitted data using a software defined radio.

Building materials:

Raspberry Pi Kit - <https://www.amazon.com/dp/B07BCC8PK7/> Software Defined Radio -

<https://www.amazon.com/dp/B011HVUEME/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Cal Poly Workshop - Simulated Satellite Communications on Raspberry Pi

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: Aerospace Vlg Workshop

Description:

Users will need to purchase own equipment before the workshop/challenge is run. (users will attempt to see simulated altitude, battery level, telemetry data from the mock satellite. It will be awesome because, we will expose participants new to the convergence of space and cybersecurity a crawl/beginner experience to gain their interest. It's designed as a workshop. The Convergence of Space & Cybersecurity Innovation.

The goal of this workshop would be to construct a “CubeSat Simulator Lite

<https://github.com/alanbjohnston/CubeSatSim/wiki> specifically

<https://github.com/alanbjohnston/CubeSatSim/wiki/CubeSat-Simulator-Lite>.

We would run through the installation of the software via a screensharing method. We'd show participants how to setup a Raspberry Pi, set up the device, install the necessary packages, attach a necessary antenna, and view the transmitted data using a software defined radio.

Building materials:

Raspberry Pi Kit - <https://www.amazon.com/dp/B07BCC8PK7/> Software Defined Radio -

<https://www.amazon.com/dp/B011HVUEME/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Cal Poly Workshop - Simulated Satellite Communications on Raspberry Pi

When: Sunday, Aug 9, 09:00 - 15:59 PDT

Where: Aerospace Vlg Workshop

Description:

Users will need to purchase own equipment before the workshop/challenge is run. (users will attempt to see simulated altitude, battery level, telemetry data from the mock satellite. It will be awesome because, we will expose participants new to the convergence of space and cybersecurity a crawl/beginner experience to gain their interest. It's designed as a workshop. The Convergence of Space & Cybersecurity Innovation.

The goal of this workshop would be to construct a “CubeSat Simulator Lite

<https://github.com/alanbjohnston/CubeSatSim/wiki> specifically

<https://github.com/alanbjohnston/CubeSatSim/wiki/CubeSat-Simulator-Lite>.

We would run through the installation of the software via a screensharing method. We'd show participants how to setup a Raspberry Pi, set up the device, install the necessary packages, attach a necessary antenna, and view the transmitted data using a software defined radio.

Building materials:

Raspberry Pi Kit - <https://www.amazon.com/dp/B07BCC8PK7/> Software Defined Radio -

<https://www.amazon.com/dp/B011HVUEME/>

Return to Index - Add to  - ics [Calendar](#) file

Title: CAN be super secure: Bit Smashing FTW

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: Car Hacking VIg 002

SpeakerBio:Brent Stone

No BIO available

Description:

Bit smashing CAN transceivers are already on the market and cost pennies. Using them would make vehicles, robots, and medical devices effectively immune from almost every layer 2 attack including denial of service. Brent explains why this security measure works so well. This is also a call to action for industries using exclusively multicast ICS protocols like CAN to invest the <\$5/platform to greatly improve their product's security.

#chv-track002-text: <https://discord.com/channels/708208267699945503/739564953014632579>

YouTube: <https://www.youtube.com/watch?v=5DYhXbWkWoA&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack002>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Can't Touch This: Detecting Lateral Movement in Zero-Touch Environments

When: Friday, Aug 7, 13:25 - 14:10 PDT

Where: Cloud Vlg

SpeakerBio: Phillip Marlow

Phillip Marlow is a cybersecurity and DevOps engineer. He helps organizations understand how to adopt DevOps practices to increase their security rather than sacrifice it in the name of speed. Phillip holds several security, cloud, and agile certifications and is currently pursuing a Master's Degree in Information Security Engineering at SANS Technology Institute.

Twitter: [@wolramp](#)

Description:

Attackers frequently use valid accounts to access servers with sensitive data. This gives them ninja-like stealth in most environments, but this session will show you how to turn the tables and use a zero-touch environment to catch them.

Zero-touch environments are a product of the fast-moving world of DevOps which is being adopted by an increasing number of successful companies including Google. This session will show that by leveraging the constraints of this environment, we can identify malicious network traffic which would otherwise blend into the noise.

This proposal is based on active research and new details may emerge during preparation of the final session. A brief overview of expected included topics:

- Why care about DevOps and Zero-Touch?
- How application servers are deployed in traditional environments
- What lateral movement with valid credentials looks like in traditional environments
- How deployment works in Zero-Touch environments
- What lateral movement with valid credentials looks like in zero-touch
- Detecting the lateral movement with existing network sensors

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Can't Touch This: Detecting Lateral Movement in Zero-Touch Environments

When: Saturday, Aug 8, 15:00 - 15:45 PDT

Where: AppSec Vlg

SpeakerBio: Phillip Marlow

Phillip Marlow is a cybersecurity and DevOps engineer. He helps organizations understand how to adopt DevOps practices to increase their security rather than sacrifice it in the name of speed. Phillip holds several security, cloud, and agile certifications and is currently pursuing a Master's Degree in Information Security Engineering at SANS Technology Institute.

Twitter: [@wolramp](#)

Description:

Zero-touch environments are a product of the fast-moving world of DevOps which is being adopted by an increasing number of successful companies. This session will show that by leveraging the constraints of this environment, we can identify malicious network traffic which would otherwise blend into the noise.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Capture The Packet (CTP)

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

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. Follow us on Twitter or Facebook (links below) to get notifications for dates and times your team will compete, as well as what prizes will be awarded.

Twitter capturetp: <https://twitter.com/capturetp>

Twitter wallofsheep: <https://twitter.com/wallofsheep>

Discord: <https://discord.com/channels/708208267699945503/711643512625430529>

Web: <https://www.capturethepacket.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Capture The Packet (CTP)

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

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. Follow us on Twitter or Facebook (links below) to get notifications for dates and times your team will compete, as well as what prizes will be awarded.

Twitter capturetp: <https://twitter.com/capturetp>

Twitter wallofsheep: <https://twitter.com/wallofsheep>

Discord: <https://discord.com/channels/708208267699945503/711643512625430529>

Web: <https://www.capturethepacket.com/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Capture The Packet (CTP)

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

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. Follow us on Twitter or Facebook (links below) to get notifications for dates and times your team will compete, as well as what prizes will be awarded.

Twitter capturetp: <https://twitter.com/capturetp>

Twitter wallofsheep: <https://twitter.com/wallofsheep>

Discord: <https://discord.com/channels/708208267699945503/711643512625430529>

Web: <https://www.capturethepacket.com/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Car (to Cloud) Talk: Using MQTT for Car Hacking

When: Friday, Aug 7, 16:00 - 16:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio:Jaime

Jaime is an EE turned software developer turned security researcher. She caught the infosec bug through playing CTFs, and now works at GRIMM hacking cars. In her spare time, she adds LEDs to things and hangs out with her dog.

Description:

As with IoT, cars are becoming increasingly "smart". In the automotive and trucking world, this means adding the ability to collect real-time telemetry data, gather information for predictive maintenance, as well as consumer features like remote lock/unlock. This talk will cover the internals of how MQTT--a lightweight messaging protocol frequently used in automotive and IoT--works, and how it's used in automotive applications.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Car (to Cloud) Talk: Using MQTT for Car Hacking

When: Saturday, Aug 8, 16:00 - 16:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio:Jaime

Jaime is an EE turned software developer turned security researcher. She caught the infosec bug through playing CTFs, and now works at GRIMM hacking cars. In her spare time, she adds LEDs to things and hangs out with her dog.

Description:

As with IoT, cars are becoming increasingly "smart". In the automotive and trucking world, this means adding the ability to collect real-time telemetry data, gather information for predictive maintenance, as well as consumer features like remote lock/unlock. This talk will cover the internals of how MQTT--a lightweight messaging protocol frequently used in automotive and IoT--works, and how it's used in automotive applications.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Car Hacking Village CTF

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Come learn, hack, play at the Car Hacking Village. The village is an open, collaborative space to hack actual vehicles that you don't have to worry about breaking! Don't have tools? We'll loan you some. Never connected to a car? We'll show you how. Don't know where the controllers are? We'll show you how to take it apart.

Additionally we'll host a Donkey Car race. Check out our web site for up to date info.

Want to race? Check out of full car simulator(s).

Want to learn more about automotive hacking and cyber security? Check out our talks.

Want to hack mobility scooters? Yes! We'll do that to.

Also, check out the CHV CTF.

Discord: <https://discord.com/channels/708208267699945503/711643596658311229>

Twitter: <https://twitter.com/CarHackVillage>

Web: <https://www.carhackingvillage.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Car Hacking Village CTF

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Come learn, hack, play at the Car Hacking Village. The village is an open, collaborative space to hack actual vehicles that you don't have to worry about breaking! Don't have tools? We'll loan you some. Never connected to a car? We'll show you how. Don't know where the controllers are? We'll show you how to take it apart.

Additionally we'll host a Donkey Car race. Check out our web site for up to date info.

Want to race? Check out of full car simulator(s).

Want to learn more about automotive hacking and cyber security? Check out our talks.

Want to hack mobility scooters? Yes! We'll do that to.

Also, check out the CHV CTF.

Discord: <https://discord.com/channels/708208267699945503/711643596658311229>

Twitter: <https://twitter.com/CarHackVillage>

Web: <https://www.carhackingvillage.com/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Car Hacking Village CTF

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Come learn, hack, play at the Car Hacking Village. The village is an open, collaborative space to hack actual vehicles that you don't have to worry about breaking! Don't have tools? We'll loan you some. Never connected to a car? We'll show you how. Don't know where the controllers are? We'll show you how to take it apart.

Additionally we'll host a Donkey Car race. Check out our web site for up to date info.

Want to race? Check out of full car simulator(s).

Want to learn more about automotive hacking and cyber security? Check out our talks.

Want to hack mobility scooters? Yes! We'll do that to.

Also, check out the CHV CTF.

Discord: <https://discord.com/channels/708208267699945503/711643596658311229>

Twitter: <https://twitter.com/CarHackVillage>

Web: <https://www.carhackingvillage.com/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Carnivore (Microsoft External Attack Tool)

When: Sunday, Aug 9, 12:00 - 13:50 PDT

Where: See Description or Village

SpeakerBio: Chris Nevin
Senior Security Consultant at NCCGroup

Description:

Carnivore is a username enumeration and password spraying tool for Microsoft services (Skype for Business, ADFS, RDWeb, Exchange and Office 365). It originally began as an on-premises Skype for Business enumeration/spray tool as I was finding that these days, organizations often seem to have locked down their implementations of Exchange, however, Skype for Business has been left externally accessible, and has not received as much attention from previous penetration tests due to the lack of tools as impactful as Mailsniper. Overtime this was improved and built upon to bring the same service discovery, username enumeration and password spraying capability to Skype, ADFS, RDWeb, Exchange, and O365 all in the same tool. Carnivore includes new post compromise functionality for Skype for Business (pulling the internal address list and user presence through the API), and smart detection of the username format for all services. As a practical means of entry into an organisation – numerous external penetration tests have uncovered an on-premises Skype for Business or ADFS server even for organisations that have moved Mail/SSO/etc to the cloud.

Audience: Offense

Interact @ #dl-nevin-carnivore-text: <https://discord.com/channels/708208267699945503/730256550442041373>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://github.com/ReverendThing/Carnivore>

Forum: <https://forum.defcon.org/node/233116>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DL - Friday - 10:00-11:50 PDT

Title: Carnivore (Microsoft External Attack Tool)

When: Friday, Aug 7, 10:00 - 11:50 PDT

Where: See Description or Village

SpeakerBio: Chris Nevin
Senior Security Consultant at NCCGroup

Description:

Carnivore is a username enumeration and password spraying tool for Microsoft services (Skype for Business, ADFS, RDWeb, Exchange and Office 365). It originally began as an on-premises Skype for Business enumeration/spray tool as I was finding that these days, organizations often seem to have locked down their implementations of Exchange, however, Skype for Business has been left externally accessible, and has not received as much attention from previous penetration tests due to the lack of tools as impactful as Mailsniper. Overtime this was improved and built upon to bring the same service discovery, username enumeration and password spraying capability to Skype, ADFS, RDWeb, Exchange, and O365 all in the same tool. Carnivore includes new post compromise functionality for Skype for Business (pulling the internal address list and user presence through the API), and smart detection of the username format for all services. As a practical means of entry into an organisation – numerous external penetration tests have uncovered an on-premises Skype for Business or ADFS server even for organisations that have moved Mail/SSO/etc to the cloud.

Audience: Offense

Interact @ #dl-nevin-carnivore-text: <https://discord.com/channels/708208267699945503/730256550442041373>

Watch @ #dl-video2-voice: <https://discord.com/channels/708208267699945503/734027778646867988>

Github: <https://github.com/ReverendThing/Carnivore>

Forum: <https://forum.defcon.org/node/233116>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Catch Me if You Can

When: Saturday, Aug 8, 07:15 - 08:15 PDT

Where: Red Team Vlg

SpeakerBio: Eduardo Arriols

Eduardo Arriols is RootPointer's Founder, a Cybersecurity Startup. Previously, he has worked for 6 years as head of Red Team teams in different organizations, coordinating and developing only advanced intrusion exercises (Red Team) at the international level (America, South America and Europe). Undergraduate and postgraduate university professor at U-tad University, where he teaches in the different courses of the Software Engineering degree. Likewise, he also teaches in different postgraduate courses at other Spanish Universities like UCLM and URJC. Author of the book "The Company's Red Team" by the 0xWord publisher (Spanish), which describes the Red Team concept, and how to run intrusion simulations on an organization at a technical level. Security researcher and speaker at national and international conferences such as RootedCON, Navaja Negra, STIC Conference (CCN-Cert) or 8.8 Security Conference (Chile and Bolivia).

Description:

The presentation will show, from a technical point of view, how to deploy backdoors to guarantee access to an organization. Initially, a brief review about types of persistence, locations where it can be deployed and common aspects to be taken into account will be carried out, to then go on to describe all the details that allow a Red Team to guarantee access to the entity without the organization being able to detect it or being able to expel the attacker before the attacker re-enters using another alternative persistence. The presentation will feature the following highlights: - General introduction to the concepts necessary to understand the details regarding the scenarios where it is necessary to deploy persistence in an organization (in real intrusion). - Reverse connection typology such as situations where there is direct access to the Internet, connection via proxy, proxy with authentication, DNS, ... - Infrastructure and techniques for persistence deployment, indicating the type of servers and advanced techniques such as Domain fronting, IP laundry, ... - Traditional deployment of persistence on an organization both in existing systems in DMZ, internal servers, workstations, Cloud servers, Active Directory, ... - Alternative persistence to guarantee unknown access through users with predictable credentials based on password history, Wireless backdoor on workstations (in both directions), extracting internal WiFi passwords, pivoting through resource reconstruction, periodic tasks to modify AD setting, monthly Outlook rules configured and upload interna GAL table of users, visual information extraction using screen and others. - Anti-forensic techniques for the deployment of persistence, to avoid the identification of these by the Security team. - Types of behavior to act and techniques when the security team detects a persistence, allowing access to the entity to be recovered before having lost access to company. The combined use of the exposed techniques and actions, as will be shown in the presentation, means that the security team does not have the ability to expel the Red Team in any case, allowing the intrusion to be carried out with greater freedom. The presentation is the result of experience in developing deep Red Team exercises on the main organizations in Spain (IBEX35), as well as large banking and industrial entities in Europe and America for more than 6 years. After the presentation, an Open Source tool will be published to help in the development of the persistence deployment.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 14:30-14:59 PDT

Title: Chairman Benjamin Hovland, US Election Assistance Commission

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: Voting VIg

SpeakerBio: Benjamin Hovland , Chairman, U.S. Election Assistance Commission

No BIO available

Description: No Description available

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Checklist For Aviation Vulnerability Disclosure: Don't Go It Alone

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: Aerospace VIg

SpeakerBio:Jay Angus

Mr. Jay Angus is a career civil servant with 16 years of experience as a federal employee. He currently serves as the federal lead for the Industrial Control Systems Vulnerability Management and Coordination program within Cybersecurity Infrastructure Security Agency. Prior to joining CISA, he worked for 10 years as an Information Assurance Manager at Naval Hospital Pensacola and SpaWar.

In his current role, he manages day to day operations within the Cybersecurity Infrastructure Security Agency ICS vulnerability disclosure program. As the federal lead for this program he provides oversight of the responsible disclosure of Industrial Control Systems, IoT equipment, and medical devices. One of the significant challenges of this mission space is developing the trust of vendors, asset owners, and researchers, while providing actionable mitigation and remediation strategies to the system owners across the sixteen critical infrastructure sectors.

Description:

Cybersecurity vulnerabilities are ever present in IT and OT systems and the aerospace sector is not exempt from these findings. What should a researcher or vendor do when they find a vulnerability? This is a common question but can have many and variety complex answers. Showing how a few simple steps by each participant in the process of coordinated disclosure can decrease the stress of the efforts and result in trust among researchers and a more resilient aviation sector.

Major points will focus on:

- What researchers should be doing in preparation of disclosure.
- When a researcher should be looking for help with coordination.
- Questions vendor should be asking in preparation of a public disclosure.
- Each disclosure is a unique event and should be leveraged to build upon.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BHV - Saturday - 16:00-16:30 PDT

Title: Chinese Military Laboratory Mission + COVID-19

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: BioHacking Vlg

SpeakerBio: The Red Dragon

No BIO available

Description:

Chinese Military Laboratory Mission + COVID-19 discusses respectful research regarding military labs in the People's Republic of China and potential implications for weaponizing viruses, such as COVID-19. Audience will receive a filled experienced trip in the Chinese Military bio-weapons programs.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

Return to Index - Add to  - ics [Calendar](#) file

Title: ChupaCarBrah: Open Source Hardware and Software for Interacting with your Vehicle CAN Bus

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: Car Hacking VIg 002

SpeakerBio: Marcelo Sacchetin

No BIO available

Description:

Commercial products for interacting with CAN can be pricey and not easily extensible. Some good open source hardware are very often out of stock by distributors. ChupaCarBrah is a Python based device for sending and receiving CAN messages from your vehicle that requires just a BeagleBone Blue and some wiring.

We cover how to build a device 100% based on open source software and hardware. It makes it more affordable, and easy to use/extend. It is designed for newcomers to the car hacking community, and also for more seasoned hackers that will be able to leverage a single board computer attached to the car's CAN bus. As an example on how to extend it, we show how to use cellular LTE network to exfiltrate all the OBDII/CAN and GPS data to the cloud. It is pretty useful specially for remotely monitoring the car, and also for online training and/or virtual meetings. All source code and detailed instructions on how to install, assemble and use the device are shared on Github and Hackster.io.

#chv-track002-text: <https://discord.com/channels/708208267699945503/739564953014632579>

YouTube: <https://www.youtube.com/watch?v=5DYhXbWkWoA&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack002>

Return to Index - Add to  - ics [Calendar](#) file

DL - Saturday - 16:00-17:55 PDT

Title: CIRCO v2: Cisco Implant Raspberry Controlled Operations

When: Saturday, Aug 8, 16:00 - 17:55 PDT

Where: See Description or Village

SpeakerBio:Emilio Couto

Emilio Couto (@ekio_jp) is a Security Consultant with more than 20 years of experience in the network and security field. Born and raised in Argentina, he is currently located in Japan where multitasking between language, culture and technologies is a must. Over the last decade focusing mainly on Finance IT and presenting tools in conferences (DEF CON, BlackHat Asia, HITB, Code Blue, AV Tokyo and SECCON). In his spare time he enjoys 3D printing, tinkering electronics and home-made IoT devices.

Twitter: @ekio_jp

Description:

Designed under Raspberry Pi and aimed for Red Team Ops, we take advantage of "Sec/Net/Dev/Ops" enterprise tools to capture network credentials in stealth mode

Audience: Offense/Hardware

Interact @ #dl-couto-circo-v2-text: <https://discord.com/channels/708208267699945503/730256145771659335>

Watch @ #dl-video2-voice: <https://discord.com/channels/708208267699945503/734027778646867988>

Github: <https://github.com/ekiojp/circo>

Forum: <https://forum.defcon.org/node/233127>

Return to Index - Add to  - ics [Calendar](#) file

Title: CIRCO v2: Cisco Implant Raspberry Controlled Operations

When: Friday, Aug 7, 10:00 - 11:50 PDT

Where: See Description or Village

SpeakerBio:Emilio Couto

Emilio Couto (@ekio_jp) is a Security Consultant with more than 20 years of experience in the network and security field. Born and raised in Argentina, he is currently located in Japan where multitasking between language, culture and technologies is a must. Over the last decade focusing mainly on Finance IT and presenting tools in conferences (DEF CON, BlackHat Asia, HITB, Code Blue, AV Tokyo and SECCON). In his spare time he enjoys 3D printing, tinkering electronics and home-made IoT devices.

Twitter: @ekio_jp

Description:

Designed under Raspberry Pi and aimed for Red Team Ops, we take advantage of "Sec/Net/Dev/Ops" enterprise tools to capture network credentials in stealth mode

Audience: Offense/Hardware

Interact @ #dl-couto-circo-v2-text: <https://discord.com/channels/708208267699945503/730256145771659335>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://github.com/ekiojp/circo>

Forum: <https://forum.defcon.org/node/233127>

Return to Index - Add to  - ics [Calendar](#) file

Title: Closing Ceremonies

When: Sunday, Aug 9, 17:00 - 17:59 PDT

Where: See Description or Village

SpeakerBio:The Dark Tangent

No BIO available

Description:

The closing ceremonies will be streamed on the DEF CON Twitch. There will be a live Q&A session during part of the event, and questions can be posted in #track-1-live-qa.

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live-qa: <https://discord.com/channels/708208267699945503/733079691145117848>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CLV - Sunday - 13:30-13:50 PDT

Title: Closing Note

When: Sunday, Aug 9, 13:30 - 13:50 PDT

Where: Cloud Vlg

Description:

YouTube: <https://www.youtube.com/watch?v=DSipgVlsAfo>

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

Return to Index - Add to  - ics [Calendar](#) file

MOV - Sunday - 15:30-15:59 PDT

Title: Closing talk

When: Sunday, Aug 9, 15:30 - 15:59 PDT

Where: Monero Vlg

SpeakerBio:rehr

No BIO available

Description:No Description available

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cloud Frontier

When: Saturday, Aug 8, 13:15 - 13:59 PDT

Where: Cloud Vlg

SpeakerBio: Setu Parimi

Setu Parimi is a Cloud Security Architect with specialization towards defense-in-depth and incident response in the cloud-native environments.

Twitter: [@setuparimi](https://twitter.com/setuparimi)

Description:

Cloud Frontier is a security monitoring tool for Internet Facing Assets in AWS, GCP, and Azure. It can be quickly deployed into AWS and will periodically enumerate internet-facing IP addresses, Domain Names, Block Storages, CDNs, and Object Storage resources from AWS, GCP, and Azure.

The results from this enumeration process are pushed into a DynamoDB and then are sent to analyzers using an asynchronous queuing system. Analyzers use Shodan, VirusTotal, URLScan.io, Mozilla Observatory, and whois to provide insights around the following:

- Web Reputation
- IP Reputation
- DNS Information
- GeoIP Information
- IP and Domain Blacklist check etc

License: MIT License

YouTube: https://www.youtube.com/watch?v=gwBG_oKDINQ

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cloud host base strategy by staging defensive tools for Threat Hunting and Forensics

When: Sunday, Aug 9, 11:00 - 11:45 PDT

Where: Cloud Vlg

SpeakerBio: Michael Mimo

No BIO available

Twitter: [@securitydevops](https://twitter.com/securitydevops)

Description:

Cloud instance forensic acquisition presents certain challenges to forensics teams. Traditional forensic methods usually are not effective in the cloud. Access and networks are designed differently than in an on-premise Data Center. Forward thinking strategies need to be implemented so that Incident Response Cyber teams can effectively use forensically sound methods to examine artifacts on hosts.

My talk is about how to prepare your organization for forensic acquisitions in a cloud infrastructure. I will quickly cover how to prepare a fleet of systems for memory and physical disk forensics. The targets are AWS EC2 instances but could be applied to any other cloud providers host provisioning infrastructure. I will focus on the process and infrastructure required to do this level of inspection. By the end you will be able to apply these strategies to activities such as Threat Hunting.

Many organizations struggle with implementing Threat Hunting programs with orchestration in mind to capture memory and disk level forensics. How does a Cyber team respond to an alert they receive from a cloud host? How can they quickly collect artifacts for further forensic inspection? Last, how can you best secure the forensics infrastructure from where you launch the orchestrated forensic examiner systems?

The first part of my talk will describe the infrastructure required to be in the place to support forensic orchestration. I will outline a strategy: servers, tools, storage, and protective measures to ensure that forensic activities are conducted behind a cloud of secrecy. Maintaining stealth mode is critically important to enabling the forensic team to do their job while the business is not impacted by the investigative activities.

In the second part, we will examine the pipeline process to implement solutions in EC2 instances with pre-configured memory and acquisition tools ready to be tapped into by the forensic team. I will discuss some of the challenges encountered when conducting forensics with the different AWS hypervisor solutions.

As a result, testing each design of the Linux instances with your forensics tools is an important part of the process. Do not expect the forensic tools to work seamlessly when the architecture teams switch fundamental infrastructure designs. Each phase of the AMI delivery pipeline needs to be tested and verified that the Cyber team can continue to perform their investigations without running into challenges during a real incident. Do not wait until forensics is really needed to only find out that the tools designed did not perform their job.

YouTube: <https://www.youtube.com/watch?v=DSipgVlsAfo>

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

Return to Index - Add to  - ics [Calendar file](#)

Title: Cloud Security Monitoring on a Dime Store Budget (Beginner)

When: Sunday, Aug 9, 13:30 - 14:59 PDT

Where: Blue Team VIg - Workshop Track 2

SpeakerBio: Wes Lambert

Wes Lambert is a Senior Engineer at Security Onion Solutions, where he helps companies to implement enterprise security monitoring solutions and better understand their computer networks. Wes is a huge fan of open source software projects, and loves to solve problems and enhance organizational security using completely free and easily deploy-able tools.

Twitter: [@therealwlambert](https://twitter.com/therealwlambert)

Description:

As organizations continue to rely on the cloud to run critical production workloads and store potentially sensitive data, it is more important than ever to understand our cloud infrastructure, and implement monitoring to assist in providing greater insight into the "goings on" of cloud environments. In this workshop, attendees will learn how they can leverage free and open source tools to enable effective network security monitoring for major cloud providers, extending their visibility, providing greater overall context with regard to their organization's network traffic, and identifying anomalies that otherwise might have gone unnoticed.

This workshop will address the following topics:

Introduction to NSM (Network Security Monitoring Concepts) - key NSM concepts will be discussed/explained Major cloud providers, and native mechanisms to facilitate network security monitoring AWS/Google Cloud

Packet mirroring - we'll discuss what packet mirroring is, and how it can be utilized Cloud provider-specific core NSM/infrastructure/networking concepts and implementation - in this section, we'll discuss the components of each cloud provider's infrastructure, and how it relates to our approach to network security monitoring

AWS
Google Cloud

Automating deployment for cloud environments - in this section, we'll discuss how to automate deployment of cloud security monitoring (for free), as well as how to quickly and easily spin up and environment for testing, academia, or even a PoC for a potential production deployment.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

CLV - Friday - 06:00-12:30 PDT

Title: Cloud Village CTF

When: Friday, Aug 7, 06:00 - 12:30 PDT

Where: See Description or Village

Description:

Registrations Open - 6 AM PDT 7th August 2020 CTF start time - August 7th 11 AM PDT

CTF close time - August 9th 12:30 PM PDT

The winners will be announced on August 9th 1:30 PM PDT at the closing note

CTF Site: <https://cloudvillagectf.co/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cloud-Native Attack Detection and Simulation.

When: Sunday, Aug 9, 12:30 - 13:30 PDT

Where: Cloud Vlg

SpeakerBio: Nick Jones

Nick Jones is the cloud security lead and a senior security consultant at F-Secure Consulting (formerly MWR InfoSecurity), where he focuses on AWS security in mature, cloud-native organisations and large enterprises. He has a number of years experience delivering offensive security assessments and services to a broad client base. When he's not delivering offensively-focused engagements, he's typically found working with clients to help them develop their security operations and attack detection capabilities.

Twitter: [@nojonesuk](https://twitter.com/nojonesuk)

Description:

The cloud brings a broad range of benefits from a security perspective, including network isolation by default, strong identity controls and unprecedented visibility. It does, however, bring many changes and unique challenges of its own when compared to an on-premise estate, with modern cloud environments make heavy use of containerisation, serverless functions and other new paradigms. As such, many of the data sources used for threat hunting and attack detection in traditional environments are no longer available. In addition, most attacks consist of abusing legitimate functionality, making it challenging at times to differentiate the malicious from the benign.

Based on first-hand experience attacking and defending large enterprises, this talk will compare and contrast the benefits and challenges of attack detection in the cloud against on-premise detection, and highlight some of the key advantages, common pitfalls and key data sources. It will also offer advice and guidance on developing your own cloud attack detection capabilities in house.

Lastly, it will present Leonidas - a cloud native toolchain that allows users to easily define, simulate and detect new attack vectors and techniques against cloud environments, all tied back to the MITRE ATT&CK framework. This will include deploying and using Leonidas, constructing and executing an attack path end-to-end, and how to implement your own test cases. It'll also cover Leonidas into your detection stack to track improvement over time and support learning and skills development within your team.

YouTube: <https://www.youtube.com/watch?v=DSipgVlsAfo>

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

Return to Index - Add to  - ics [Calendar](#) file

Title: Cluster fuzz!

When: Friday, Aug 7, 13:00 - 13:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Mintynet

Network / security architect that has a passion for car hacking, found vulnerabilities in his own car and also private Car bug bounties. Now runs Car Hacking Village UK and is part of the team behind CHV at defcon

LinkedIn <https://www.linkedin.com/in/mintynet/> Twitter: <https://twitter.com/mintynet>

Website: www.mintynet.com

Twitter: [@mintynet](https://twitter.com/mintynet)

Description:

How to get started in #carhacking using cheap CAN hardware and an instrument cluster, shows the hardware needed and an example of a cluster. Then show some fuzzing of the cluster, including some tips for the CTF.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cluster fuzz!

When: Saturday, Aug 8, 13:00 - 13:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Mintynet

Network / security architect that has a passion for car hacking, found vulnerabilities in his own car and also private Car bug bounties. Now runs Car Hacking Village UK and is part of the team behind CHV at defcon

LinkedIn <https://www.linkedin.com/in/mintynet/> Twitter: <https://twitter.com/mintynet>

Website: www.mintynet.com

Twitter: [@mintynet](https://twitter.com/mintynet)

Description:

How to get started in #carhacking using cheap CAN hardware and an instrument cluster, shows the hardware needed and an example of a cluster. Then show some fuzzing of the cluster, including some tips for the CTF.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CMAP: Open Source Vehicle Services Mapping Tool for noobs

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: Car Hacking Vlg 001

SpeakerBio: Robert Leale (CarFuCar)

Robert Leale (@carfucar) is an automotive hacker and a founding member of the Car Hacking Village. For more information please visit carhackingvillage.com/about

Twitter: [@carfucar](https://twitter.com/carfucar)

Description:

CMAP works to catalog open services on vehicle Ex is by using the Diagnostic Scanning to automatically capture as much information as possible from your vehicle.

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUej1Q&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CMD+CTRL CyberRange

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

CMD+CTRL has evolved! Slip into an immersive scenario, spanning an entire corporate cloud environment. Intelligent chatbots acting as skilled hackers will guide you every step of the way, as you perform recon, social engineering, data exfiltration, privilege escalation and much more. Move through websites, servers, accounts and cloud services, all in an effort to thwart an evil CEO and corrupt corporation. Just don't get caught, or you may have to burn it all down to cover your tracks!

Forum: <https://forum.defcon.org/node/231474>

Discord: <https://discord.com/channels/708208267699945503/711643642388807800>

Twitter: <https://twitter.com/SecInnovation>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: CMD+CTRL CyberRange

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

CMD+CTRL has evolved! Slip into an immersive scenario, spanning an entire corporate cloud environment. Intelligent chatbots acting as skilled hackers will guide you every step of the way, as you perform recon, social engineering, data exfiltration, privilege escalation and much more. Move through websites, servers, accounts and cloud services, all in an effort to thwart an evil CEO and corrupt corporation. Just don't get caught, or you may have to burn it all down to cover your tracks!

Forum: <https://forum.defcon.org/node/231474>

Discord: <https://discord.com/channels/708208267699945503/711643642388807800>

Twitter: <https://twitter.com/SecInnovation>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: CMD+CTRL CyberRange

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

CMD+CTRL has evolved! Slip into an immersive scenario, spanning an entire corporate cloud environment. Intelligent chatbots acting as skilled hackers will guide you every step of the way, as you perform recon, social engineering, data exfiltration, privilege escalation and much more. Move through websites, servers, accounts and cloud services, all in an effort to thwart an evil CEO and corrupt corporation. Just don't get caught, or you may have to burn it all down to cover your tracks!

Forum: <https://forum.defcon.org/node/231474>

Discord: <https://discord.com/channels/708208267699945503/711643642388807800>

Twitter: <https://twitter.com/SecInnovation>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Coindroids

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The year is 20X5 and humanity has fallen: now there are only Coindroids. The machines we designed to manage our finances have supplanted and destroyed the human race by turning our own economy against us. Now they battle each other in the ruins of our fallen cities, driven by a single directive: money is power.

Battle your way to the top of the leaderboard by attacking rival droids and completing hidden challenges.

New to cryptocurrencies? No DEFCON to play with? Not a problem! Just come visit our booth in the contest area and we can help get you started.

Forum: <https://forum.defcon.org/node/233033>

Discord: <https://discord.com/channels/708208267699945503/711643539573833878>

Twitter: <https://twitter.com/coindroids>

Web: <https://www.coindroids.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Coindroids

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The year is 20X5 and humanity has fallen: now there are only Coindroids. The machines we designed to manage our finances have supplanted and destroyed the human race by turning our own economy against us. Now they battle each other in the ruins of our fallen cities, driven by a single directive: money is power.

Battle your way to the top of the leaderboard by attacking rival droids and completing hidden challenges.

New to cryptocurrencies? No DEFCON to play with? Not a problem! Just come visit our booth in the contest area and we can help get you started.

Forum: <https://forum.defcon.org/node/233033>

Discord: <https://discord.com/channels/708208267699945503/711643539573833878>

Twitter: <https://twitter.com/coindroids>

Web: <https://www.coindroids.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Coindroids

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The year is 20X5 and humanity has fallen: now there are only Coindroids. The machines we designed to manage our finances have supplanted and destroyed the human race by turning our own economy against us. Now they battle each other in the ruins of our fallen cities, driven by a single directive: money is power.

Battle your way to the top of the leaderboard by attacking rival droids and completing hidden challenges.

New to cryptocurrencies? No DEFCON to play with? Not a problem! Just come visit our booth in the contest area and we can help get you started.

Forum: <https://forum.defcon.org/node/233033>

Discord: <https://discord.com/channels/708208267699945503/711643539573833878>

Twitter: <https://twitter.com/coindroids>

Web: <https://www.coindroids.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Combining notebooks, datasets, and cloud for the ultimate automation factory

When: Thursday, Aug 6, 13:00 - 13:59 PDT

Where: Red Team VIg

SpeakerBio:Ryan Elkins

Ryan Elkins leads the cloud security architecture program for Eli Lilly and Company. Elkins has over 12 years of security experience leading programs across the financial, insurance, and pharmaceutical industries. Throughout his career, he has developed cloud and application security programs, managed a global security services center, performed security consulting, and has led a global information security program. Elkins holds the CISSP and CCSP certifications, a bachelors degree in Computer Technology, and a masters degree in Information Security.

Description:

The technological landscape is rapidly transforming into a data driven, automated, and measured ecosystem. Cloud is an enabler for businesses to become more agile, scalable, and global to maintain a competitive advantage. There are numerous opportunities for red teamers to adopt these same modern strategies to level up their skills, platforms, and yes, even reporting. Attendees will learn how to begin integrating cloud capabilities, scientific notebooks, and aggregated datasets into a highly efficient operating model. We will walkthrough cloud technologies including AWS SageMaker, Athena, Lambda, and API Gateway to build an end-to-end ecosystem of automation. This session will provide demos, accelerators, and code releases to make both routine processes and innovative techniques faster, repeatable, and scalable. "

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Saturday - 09:45-10:45 PDT

Title: Confessions of an Offensive ICS Cyber Security Researcher

When: Saturday, Aug 8, 09:45 - 10:45 PDT

Where: ICS Vlg

SpeakerBio: Marina Krotofil

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cons and Careers

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Career Hacking Vlg

SpeakerBio: Steven Bernstein

No BIO available

Description:

When I got my first job out in the real world, I thought: this is it: All I'm ever going to need to know for my career, for my job. Got a rude awakening that was one of those worthwhile lessons taught outside of school: invest in becoming a lifelong learner. How do you come across new ideas to keep things fresh? To borrow a saying, if you're the smartest person in the room, you're in the wrong room! Attending conferences is one way to learn about different viewpoints. Revisiting ideas is one way to renew our minds and impact the way we think. Peeking into points along a career path will demonstrate an approach to keeping an eye on constant growth, while watching out for warning signs for burn out. Compete against yourself and you'll Maybe it was the dialog in the scene or suddenly understanding what the writer must have been thinking. The point is, the introduction of new ideas is essential to keep adding value to ourselves and the things we do

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cotopaxi: IoT Protocols Security Testing Toolkit

When: Saturday, Aug 8, 16:00 - 17:55 PDT

Where: See Description or Village

SpeakerBio: Jakub Botwicz

Jakub Botwicz works as a Principal Security Engineer at Samsung Poland R&D Center leading a team of security researchers. He has more than 15 years of experience in information security and previously worked in one of the worlds leading payment card service providers, Big4 consulting company and vendor of network encryption devices. Jakub holds a PhD degree from Warsaw University of Technology and security community certificates including: GWAPT, CISSP, ECSA. Currently, he works providing security assessments (static and dynamic analysis) of different mobile and IoT components.

Description:

Cotopaxi is a set of tools for security testing of Internet of Things devices using specific network IoT/IIoT/M2M protocols (e.g. AMQP, CoAP, MQTT, DTLS, mDNS, QUIC).

Audience: IoT, AppSec

Interact @ #dl-botwicz-cotopaxi-text: <https://discord.com/channels/708208267699945503/730256477792632924>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://github.com/Samsung/cotopaxi/>

Forum: <https://forum.defcon.org/node/233117>

Return to Index - Add to  - ics [Calendar](#) file

Title: COVID 1984_ Propaganda and Surveillance during a Pandemic

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: Recon VIg

SpeakerBio:Mauro Cáseres

Mauro Cáseres (@mauroeldritch) is an argentine hacker and speaker. He spoke at DEF CON 26 Las Vegas (Recon & Data Duplication Villages), DevFest Siberia, DragonJAR Colombia, Roadsec Brasil, and DC7831 Nizhny Novgorod. Currently working as SecOps for the Argentine Ministry of Production.

Twitter: [@mauroeldritch](https://twitter.com/mauroeldritch)

Description:

What does a propaganda apparatus look like from the inside? How do groups dedicated to setting trends and censoring the opposition act? What if your government forces you to install an app that tracks you during the pandemic? What if we infiltrate a sock puppet account to understand all this better?

The official political propaganda and digital surveillance in Argentina are not new. However, in the last fifteen years, both phenomena have adopted in their favor a new technological approach worthy of study, with the emergence of companies dedicated to manufacturing online trends; cyber militancy groups aimed at setting up debates, responding to them or denouncing rival trends in a coordinated way; the project to establish an exclusive social network for pro-government and “against the establishment” militants (sponsored by the Government itself); the rise of state digital surveillance after the implementation of a Cyber ©©Patrol Protocol, and the permanent monitoring of citizens through a mandatory mobile government application during the COVID-19 Pandemic. This work aims not only to review the previous events, but also to detail the two greatest milestones of political propaganda and digital surveillance in Argentina today: the political propaganda apparatus on social networks and the digital privacy abuses caused by the government application CUIDAR-COVID19 (ar.gob.coronavirus).

For the first case, a fictitious account (sock puppet) will be infiltrated within the propaganda apparatus on social networks to achieve a detailed technical dissection of its entire operation (including its interventions and actors). Our own cyber intelligence tool, Venator.lua, will be used to obtain and process data. The following section will be devoted to the study of privacy abuses caused by the mandatory government application CUIDAR-COVID19, reverse engineering it and analyzing its source code.

Recon Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/c/ReconVillage>

#rv-talks-text: <https://discord.com/channels/708208267699945503/737048009732522014>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AEV - Friday - 12:00-17:59 PDT

Title: CPX SimpleSat

When: Friday, Aug 7, 12:00 - 17:59 PDT

Where: Aerospace VIg Workshop

Description:

Can you Hack-A-Sat? You won't know until you try! Intended for noobs, CPX SimpleSat was built to allow you to experiment with attacking a mock satellite through a ground station, mimicking the types of commands used in Hack-a-Sat to gain control of the Satellite. No previous experience required. Just curiosity and a willingness to learn!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CPX SimpleSat

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

Can you Hack-A-Sat? You won't know until you try! Intended for noobs, CPX SimpleSat was built to allow you to experiment with attacking a mock satellite through a ground station, mimicking the types of commands used in Hack-a-Sat to gain control of the Satellite. No previous experience required. Just curiosity and a willingness to learn!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: CPX SimpleSat

When: Sunday, Aug 9, 09:00 - 13:59 PDT

Where: Aerospace Vlg Workshop

Description:

Can you Hack-A-Sat? You won't know until you try! Intended for noobs, CPX SimpleSat was built to allow you to experiment with attacking a mock satellite through a ground station, mimicking the types of commands used in Hack-a-Sat to gain control of the Satellite. No previous experience required. Just curiosity and a willingness to learn!

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Crack Me If You Can (CMIYC)

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

In its tenth year, the premier password cracking contest "Crack Me If You Can" is returning to DEFCON. The world's best password cracking teams are assembled and are awaiting the hardest 48 hours of their year.

Every year, the contest has a different surprise/twist. One year it was all international passwords, last year it was password rotation and BCRYPT, and 10 years ago it was capital letters. Oh the humanity!

This year the teams will be cracking hashes, generated by the CMIYC team, using plain-texts donated by famous hackers and Internet founders. Time for you to test your password cracking skills against your heroes.

Teams have 48 hours to crack as many passwords as possible using what ever resources they can legally assemble. Teams are split into "PRO" (for the large, professional password cracking teams) and "STREET" for smaller teams, or beginners.

Each year the "Crack Me If You Can" team gives away hundreds of free password cracking shirts in the Contest area.

Forum: <https://forum.defcon.org/node/231475>

Discord: <https://discord.com/channels/708208267699945503/711644827053457478>

Twitter: <https://twitter.com/CrackMelfYouCan>

Web: <https://contest-2020.korelogic.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Crack Me If You Can (CMIYC)

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

In its tenth year, the premier password cracking contest "Crack Me If You Can" is returning to DEFCON. The world's best password cracking teams are assembled and are awaiting the hardest 48 hours of their year.

Every year, the contest has a different surprise/twist. One year it was all international passwords, last year it was password rotation and BCRYPT, and 10 years ago it was capital letters. Oh the humanity!

This year the teams will be cracking hashes, generated by the CMIYC team, using plain-texts donated by famous hackers and Internet founders. Time for you to test your password cracking skills against your heroes.

Teams have 48 hours to crack as many passwords as possible using what ever resources they can legally assemble. Teams are split into "PRO" (for the large, professional password cracking teams) and "STREET" for smaller teams, or beginners.

Each year the "Crack Me If You Can" team gives away hundreds of free password cracking shirts in the Contest area.

Forum: <https://forum.defcon.org/node/231475>

Discord: <https://discord.com/channels/708208267699945503/711644827053457478>

Twitter: <https://twitter.com/CrackMeIfYouCan>

Web: <https://contest-2020.korelogic.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Crack Me If You Can (CMIYC)

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

In its tenth year, the premier password cracking contest "Crack Me If You Can" is returning to DEFCON. The world's best password cracking teams are assembled and are awaiting the hardest 48 hours of their year.

Every year, the contest has a different surprise/twist. One year it was all international passwords, last year it was password rotation and BCRYPT, and 10 years ago it was capital letters. Oh the humanity!

This year the teams will be cracking hashes, generated by the CMIYC team, using plain-texts donated by famous hackers and Internet founders. Time for you to test your password cracking skills against your heroes.

Teams have 48 hours to crack as many passwords as possible using what ever resources they can legally assemble. Teams are split into "PRO" (for the large, professional password cracking teams) and "STREET" for smaller teams, or beginners.

Each year the "Crack Me If You Can" team gives away hundreds of free password cracking shirts in the Contest area.

Forum: <https://forum.defcon.org/node/231475>

Discord: <https://discord.com/channels/708208267699945503/711644827053457478>

Twitter: <https://twitter.com/CrackMeIfYouCan>

Web: <https://contest-2020.korelogic.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Saturday - 21:00-21:59 PDT

Title: Cracking at Extreme Scale: The Evolution of Hashstack (Rebroadcast)

When: Saturday, Aug 8, 21:00 - 21:59 PDT

Where: Password Vlg

SpeakerBio: Jeremi M Gosney (epixoip)

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Saturday - 10:00-10:59 PDT

Title: Cracking at Extreme Scale: The Evolution of Hashstack

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Password Vlg

SpeakerBio: Jeremi M Gosney (epixoip)

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Friday - 14:00-14:59 PDT

Title: Creating a decentralized storage for Kubernetes with Tardigrade and Velero

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Blockchain VIg

SpeakerBio:Kevin Leffew

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Critical Aerospace Cybersecurity: How Hacking And Designing Aerospace Systems Is Changing

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: Aerospace VIg

Speakers: Lawrence Rowell, Nathalie Feyt, Yannick Le Ray

SpeakerBio: Lawrence Rowell

Lawrence Rowell is the Product Security Officer for Thales Inflyt Experience. His responsibilities include cybersecurity governance, strategy and risk management for all business line products. He supports the continuous integration of cybersecurity in the product lifecycle from development to ongoing operations. He leads the cybersecurity product roadmap that includes new cybersecurity features and offerings. Lawrence also has 15 years of experience with cybersecurity in the finance industry, leading the cybersecurity program for a fortune 500 financial company. He graduated with an MS in Telecommunications Management from Oklahoma State University.

SpeakerBio: Nathalie Feyt

Nathalie Feyt - has worldwide responsibility of security activities for Thales Avionics, as Chief Product Security Officer. She leads the security solutions roadmap for the Thales aviation portfolio covering both airborne and ground operation systems to develop new generations of safe and secure avionics, enabling in-flight connectivity and digitalization of aviation operations. She also supports the governance of cybersecurity risks for products in operations. At a European policy level, she is the Chair of Cybersecurity for the ASD taskforce, and at the national level for France she is the Technical Expert Referee for Thales at Conseil de Cybersécurité du Transport Aérien.

SpeakerBio: Yannick Le Ray

Yannick Le Ray is an engineering graduate from Ecole Polytechnique of Montreal. He joined Thales in 2003 where he held a number of positions in bid and product management for air defence command & control systems as well as communication intelligence. Since 2018, Yannick has the worldwide responsibility of cybersecurity for the Thales aeronautics vertical including Air Traffic Management, Avionics & Airports.

Description:

Aerospace is changing – Its digital transformation must now be synonymous with being cyber secure. In-cabin systems are looking more like your everyday living room and the numerous potential entry points must be tested for security. During this session we will take you through the offensive testing that we put systems through to show you what is happening to improve the life cycle of aviation systems thanks to cybersecurity-by-design principles influenced by a hack/fix process.

From design to operation, blue teams and red teams are working together for a first line of defense to help identify vulnerabilities and ensure more robust and resilient systems – systems which we all rely on, and must be certified by Airworthiness Authorities when safety is at stake.

Join Nathalie Feyt, Lawrence Rowell and Yannick Le Ray as they lead a presentation on securing avionics, passenger systems, and air traffic management systems, and show how industry designs, attacks, learns and improves aerospace systems.

This event will be coordinated on the DEF CON Discord server, in channel #av-space-text.

Discord: <https://discord.com/channels/708208267699945503/732394328105943180>

Return to Index - Add to  - ics [Calendar](#) file

BCV - Friday - 13:00-13:30 PDT

Title: Cryptocurrencies have superusers?

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: Blockchain VIg

SpeakerBio:Mark Nesbitt

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cybersecurity informed consent for medical devices

When: Friday, Aug 7, 16:15 - 16:45 PDT

Where: BioHacking Vlg

Description:

Building on conversation within the Biohacking Village at DEFCON 27, and expertise in clinical care and implementation science (Dameff, Doerr, Tully), cybersecurity in healthcare (Coravos, Dameff, Tully), device policy and regulation (Coravos, Doerr), and informed consent (Doerr), we have defined a framework for “cybersecurity informed consent, (CIC) a platform we hope will help directly address the patient (and clinician) awareness gap of the cybersecurity vulnerabilities of connected devices, enhancing the ecosystem of trust.(Tully, et al., 2020) In February 2020, we convened a 30-person advisory team comprised of white hat hackers, clinicians, and device makers focused on identifying potentially appropriate clinical scenarios for a demonstration of CIC, informed by legal and policy research performed by Science & Society Certificate Capstone students from Duke University (phase 2). We will present an overview of this work for comment and discussion as we move into the third phase of our project: implementation and assessment of CIC within the clinic.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Cybersecurity Lessons Learned From Human Spaceflight

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: Aerospace VIg

SpeakerBio:Pam Melroy

Pam Melroy is a retired US Air Force test pilot and former NASA astronaut and Space Shuttle commander. After NASA she worked at Lockheed Martin on the Orion lunar exploration vehicle program, the Federal Aviation Administration's Office of Commercial Space Transportation, and at DARPA. She is now an independent consultant and advisor.

Description:

Space is incredibly important in our daily lives – providing the GPS navigation on our phone and in our financial system, national security communications throughout the world, and remote sensing of weather conditions and other indicators of the health of the Earth. We've had a very complacent attitude about our satellites because physical access has been impossible. Now we know our key infrastructure is at threat on the ground, and it is in space as well from both physical and cyber threats. There are many important lessons to be learned about the software approach to human space flight and its high standards for software error rate and redundancy, tiered levels of access, distributed architecture, command protocols, and there are mistakes to learn from as well. The space industry is changing very rapidly. With commercial space stations, lunar exploration, and nation states competing for achievements – and resources – in space, we must understand the implications and prepare for the challenges ahead.

This event will be coordinated on the DEF CON Discord server, in channel #av-space-text.

Discord: <https://discord.com/channels/708208267699945503/732394328105943180>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Cybersecurity Meets Aviation Regulation

When: Sunday, Aug 9, 15:00 - 15:59 PDT

Where: Aerospace Vlg

Speakers: Aaron Cornelius, Tim Brom

SpeakerBio: Aaron Cornelius

Aaron Cornelius is a Senior Security Researcher at GRIMM specializing in the security of automotive, aerospace, critical infrastructure and industrial control systems. Aaron has over 15 years developing embedded and safety critical systems for telecom, aviation, medical, and industrial applications.

SpeakerBio: Tim Brom

Tim Brom is the Managing, Senior Security Researcher for Embedded Systems at GRIMM specializing in automotive security research. Tim has over ten years experience as a software developer and security researcher with a focus on automotive, aerospace, critical infrastructure and industrial control systems. Additionally, Tim has contributed extensively to the development of CanCat, GRIMM's open source CAN bus reverse-engineering tool, and CANT, a tool for interacting with CAN bus at the electrical layer. Tim was the lead engineer in the development of GRIMM's car-hacking workbenches. Tim has also had publications about car-hacking tools and techniques, including on the Macchina M2.

Description:

Software development for aviation is highly regulated, and process driven. The current processes, as defined in DO-178C and related standards, originate from a history of designing and testing mechanical components. In the past you designed a part and once installed it only had to be monitored for physical condition. It was assumed that maintenance procedures would be able to identify which components are in flight condition and which are not. But now that there are USB ports and iPads in the cockpit, do these previous assumptions remain valid? How can we ensure that flight systems are not compromised after being installed? What can be done to help ensure aviation systems are secure?

There are 4 primary areas of concern on a modern aircraft: - Maintenance interfaces - What is necessary to ensure that software communicating with the aircraft is correct and operates in a secure manner? - Passenger interfaces - What is necessary to ensure that systems passengers interact with cannot interfere with the aircraft operation? - Crew accessible interfaces - What is necessary to ensure that the crew cannot accidentally connect a malicious device to flight systems? - Pre-flight software validation - Is there a procedure that could be used to ensure that the software running on aircraft systems is 100% correct and unmodified?

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Cypher for Defenders: Leveraging Bloodhound Data Beyond the UI (Intermediate)

When: Friday, Aug 7, 10:00 - 11:30 PDT

Where: Blue Team VIg - Workshop Track 1

SpeakerBio:Scoubi

Mathieu Saulnier is a “Security Enthusiast ©@h3xstream. He has held numerous positions as a consultant within several of Quebec’s largest institutions. For the last 8 years he has been focused on putting in place a few SOC and has specialized in detection (Blue Team), content creation and mentorship. He worked as a † Senior Security Architect » and acted as “Adversary Detection Team Lead and “Threat Hunting Team Lead for one of Canada’s largest carrier for many years and is now SOC Team Lead in a large financial institution. He loves to give talk and had the honor to do so at GoSec, BSidesCharm, NorthSec, BSidesLV, Defcon’s BTV and Derbycon.

Twitter: @ScoubiMtl

Description:

Bloodhound stores AD data in a Neo4j. The UI allows you to get some information out of the box, but that is only the tip of the iceberg. Using Cypher if you can think it, you can visualize it!

The workshop will start with a quick presentation of BloodHound (BH). This is to make sure everybody understands the product as I very often meet security practitioners that never heard of the tool. (5 minutes)

The participants will be provided with test data, either in JSON format (a few KB) that can import in the BH UI or as a Neo4j database (very big). The reason to provide both is that BH is now detected by many AV as a Hacking tool and I don't want to exclude participants who come with their work computer. Those files will be provided ahead of time via Dropbox or similar file sharing site.

The first part of the workshop will go over the various objects present in BH: Computers, Groups, OU, Domains, etc. and the properties of those objects. We will learn how to interact with them using both the UI and the Neo4j Web Console (NWC). We will then use the prebuilt queries from the BH UI and use them in the NWC. From there we will start modifying them and see what impact it has. Debugging techniques will be shown. (~20 minutes)

After that we will go into a bit more advance query type, for example multiple relationships and chaining queries together. A few examples will be provided and the participants will be able to replicate the queries and see the result. (~30 minutes)

Finally, the participants will receive a list of questions and they will need to build the Cypher Queries themselves in order to find the answer. I will be there to assist them and debug their queries as needed. (~30 minutes)

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: D0 N0 H4RM: A Healthcare Security Conversation

When: Friday, Aug 7, 20:00 - 20:59 PDT

Where: DEF CON Fireside Twitch

Speakers: Ash Luft, Christian “quaddi Dameff, Jeff “r3plicant Tully, Suzanne Schwartz, Vidya Murthy

SpeakerBio: Ash Luft , Software Engineer Starfish Medical

Ash Luft is an Embedded Software Engineer with a background in Computer Science, Biochemistry, and Electrical Engineering. With industry experience in Software and Biomedical Device Development, Ash specializes in designing for and implementing safety, security, and privacy in Clinical IoT and Medical Devices. Ash is passionate about protecting patient outcomes while delivering cost-effective, high quality solutions.

SpeakerBio: Christian “quaddi Dameff , MD, Physician & Medical Director of Security at The University of California San Diego

Christian (quaddi) Dameff MD is an Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate) at the University of California San Diego. He is also a hacker, former open capture the flag champion, and prior DEF CON/RSA/Blackhat/HIMSS speaker. Published works include topics such as therapeutic hypothermia after cardiac arrest, novel drug targets for myocardial infarction patients, and other Emergency Medicine related works with an emphasis on CPR optimization. Published security research topics including hacking critical healthcare infrastructure, medical devices and the effects of malware on patient care. This is his sixteenth DEF CON.

Twitter: [@CDameffMD](#)

SpeakerBio: Jeff “r3plicant Tully , MD, Anesthesiologist at The University of California Davis

Jeff (r3plicant) Tully is an anesthesiologist, pediatrician and security researcher with an interest in understanding the ever-growing intersections between healthcare and technology.

Twitter: [@JeffTullyMD](#)

SpeakerBio: Suzanne Schwartz , MD, Associate Director for Science and Strategic Partnerships at the US Food and Drug Administration FDA

Dr. Suzanne Schwartz’s programmatic efforts in medical device cybersecurity extend beyond incident response to include raising awareness, educating, outreach, partnering and coalition-building within the Healthcare and Public Health Sector (HPH) as well as fostering collaborations across other government agencies and the private sector. Suzanne has been recognized for Excellence in Innovation at FDA’s Women’s History Month on March 1st 2018 for her work in Medical Device Cybersecurity. Suzanne chairs CDRH’s Cybersecurity Working Group, tasked with formulating FDA’s medical device cybersecurity policy. She also co-chairs the Government Coordinating Council (GCC) for the HPH Critical Infrastructure Sector, focusing on the sector’s healthcare cybersecurity initiatives.

SpeakerBio: Vidya Murthy , Vice President Operations, MedCrypt

Vidya is fascinated by the impact of cybersecurity on the healthcare space. Beginning her career in consulting, she realized a passion for healthcare and worked for global medical device manufacturer Becton Dickinson. She has since joined MedCrypt, a company focused on bringing cybersecurity leading practices to medical device manufacturers. Vidya holds an MBA from the Wharton School.

Description:

It is certainly a time of discovery- though the truths revealed by the COVID-19 crisis can be bitter and bleak. At a time when all attention is focused on the ERs and ICUs that make up the battle’s front lines, it is easy to cast aside old warnings to focus solely on the clinical war. But the need for safety and security only increases in the face of a pandemic- and healthcare cybersecurity is no different. From testing to ventilators, every facet of our response to COVID-19 depends on trustworthy and reliable technology.

Title: Darknet Contest

When: Thursday, Aug 6, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Here at Darknet, We are a Real Life (RL) Massively Multiplayer Online Role Playing Game (MMORPG), where we teach you real life skills and you get in-game points for it. Some may call this Gamified learning. We assume no prior knowledge on a subject, teach you the basics, then challenge you to use what you have learned. Our contest has a range of quests, starting with simple tasks and working your way up to very complex problems.

In the past we have taught you how to lock pick, crack wifi, create a PGP Key and communicate online safely, as well as soldering, programming, and code cracking, just to name a few. From there we would have sent you on quests to go to the different villages to learn something from them, and then come back and test your skills.

But alas, we have been forced underground... And while the physical aspect of the conference has moved online, so have we. This year we will be focusing on the skills you will learn, past skills you will refresh, and your interactions with the community. There will not be a points scoreboard this year. Many of you who have previously bought the Darknet 8 Badge have not unlocked the full features. We have quests for you to learn how to interact, develop, and reprogram it. It's time to Learn, Teach, and Play Agents, are you ready?

Info: <https://dcdark.net/>

Discord: <https://discordapp.com/channels/708208267699945503/735849065593438248/737077762845704224>

Twitter DCDarkNet: <https://twitter.com/DCDarknet>

Twitter Holon: https://twitter.com/Holon_Network

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Darknet Contest

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Here at Darknet, We are a Real Life (RL) Massively Multiplayer Online Role Playing Game (MMORPG), where we teach you real life skills and you get in-game points for it. Some may call this Gamified learning. We assume no prior knowledge on a subject, teach you the basics, then challenge you to use what you have learned. Our contest has a range of quests, starting with simple tasks and working your way up to very complex problems.

In the past we have taught you how to lock pick, crack wifi, create a PGP Key and communicate online safely, as well as soldering, programming, and code cracking, just to name a few. From there we would have sent you on quests to go to the different villages to learn something from them, and then come back and test your skills.

But alas, we have been forced underground... And while the physical aspect of the conference has moved online, so have we. This year we will be focusing on the skills you will learn, past skills you will refresh, and your interactions with the community. There will not be a points scoreboard this year. Many of you who have previously bought the Darknet 8 Badge have not unlocked the full features. We have quests for you to learn how to interact, develop, and reprogram it. It's time to Learn, Teach, and Play Agents, are you ready?

Info: <https://dcdark.net/>

Discord: <https://discordapp.com/channels/708208267699945503/735849065593438248/737077762845704224>

Twitter DCDarkNet: <https://twitter.com/DCDarknet>

Twitter Holon: https://twitter.com/Holon_Network

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Darknet Contest

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Here at Darknet, We are a Real Life (RL) Massively Multiplayer Online Role Playing Game (MMORPG), where we teach you real life skills and you get in-game points for it. Some may call this Gamified learning. We assume no prior knowledge on a subject, teach you the basics, then challenge you to use what you have learned. Our contest has a range of quests, starting with simple tasks and working your way up to very complex problems.

In the past we have taught you how to lock pick, crack wifi, create a PGP Key and communicate online safely, as well as soldering, programming, and code cracking, just to name a few. From there we would have sent you on quests to go to the different villages to learn something from them, and then come back and test your skills.

But alas, we have been forced underground... And while the physical aspect of the conference has moved online, so have we. This year we will be focusing on the skills you will learn, past skills you will refresh, and your interactions with the community. There will not be a points scoreboard this year. Many of you who have previously bought the Darknet 8 Badge have not unlocked the full features. We have quests for you to learn how to interact, develop, and reprogram it. It's time to Learn, Teach, and Play Agents, are you ready?

Info: <https://dcdark.net/>

Discord: <https://discordapp.com/channels/708208267699945503/735849065593438248/737077762845704224>

Twitter DCDarkNet: <https://twitter.com/DCDarknet>

Twitter Holon: https://twitter.com/Holon_Network

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Darknet Contest

When: Sunday, Aug 9, 09:00 - 11:59 PDT

Where: See Description or Village

Description:

Here at Darknet, We are a Real Life (RL) Massively Multiplayer Online Role Playing Game (MMORPG), where we teach you real life skills and you get in-game points for it. Some may call this Gamified learning. We assume no prior knowledge on a subject, teach you the basics, then challenge you to use what you have learned. Our contest has a range of quests, starting with simple tasks and working your way up to very complex problems.

In the past we have taught you how to lock pick, crack wifi, create a PGP Key and communicate online safely, as well as soldering, programming, and code cracking, just to name a few. From there we would have sent you on quests to go to the different villages to learn something from them, and then come back and test your skills.

But alas, we have been forced underground... And while the physical aspect of the conference has moved online, so have we. This year we will be focusing on the skills you will learn, past skills you will refresh, and your interactions with the community. There will not be a points scoreboard this year. Many of you who have previously bought the Darknet 8 Badge have not unlocked the full features. We have quests for you to learn how to interact, develop, and reprogram it. It's time to Learn, Teach, and Play Agents, are you ready?

Info: <https://dcdark.net/>

Discord: <https://discordapp.com/channels/708208267699945503/735849065593438248/737077762845704224>

Twitter DCDarkNet: <https://twitter.com/DCDarknet>

Twitter Holon: https://twitter.com/Holon_Network

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Data Analysis for Detection Research Through Jupyter Notebooks 101 (Beginner)

When: Friday, Aug 7, 18:00 - 19:30 PDT

Where: Blue Team VIg - Workshop Track 2

Speakers:Roberto Rodriguez,Jose Rodriguez

SpeakerBio:Roberto Rodriguez

Roberto Rodriguez is a threat researcher and security engineer at the Microsoft Threat Intelligence Center (MSTIC) R&D team.

He is also the author of several open source projects, such as the Threat Hunter Playbook, Mordor, OSSEM, HELK and others, to aid the community development of techniques and tooling for threat research. He is also the founder of a new community movement to empower others in the InfoSec community named Open Threat Research.

Blog at <https://medium.com/@Cyb3rWard0g>

Twitter: [@Cyb3rWard0g](https://twitter.com/Cyb3rWard0g)

<https://medium.com/@Cyb3rWard0g>

SpeakerBio:Jose Rodriguez

Jose is currently part of the ATT&CK team where he is currently revamping the concept of data sources. He is also one of the founders of Open Threat Research (OTR) and author of open source projects such as Infosec Jupyter Book, Open Source Security Event Metadata (OSSEM), Mordor, and Openhunt.

Twitter: [@Cyb3rPandaH](https://twitter.com/Cyb3rPandaH)

Description:

Please see <https://cfc.blueteamvillage.org/call-for-content-2020/talk/GCUYNN/> for pre-reqs.

From a detection research perspective, even after learning how to simulate a threat actor technique and generate some data in your lab environment, you might still struggle to know what to do with it. In some cases, you might need to filter, transform, correlate and visualize your data to come up with the right detection logic. In this workshop, we will walk you through a few basic data analysis techniques using open source and SIEM agnostic tools such as Jupyter Notebooks which are not only used by large organizations, but also can be deployed at home for free. Pre Requirements

Basics of Python

(optional) A computer with Docker Installed. If you are planning on deploying Jupyter in your own system, we will show you how to deploy it via Docker. It is not necessary since we are going to use BinderHub to interact with Jupyter Notebooks throughout the whole workshop.

Outline

Introduction to Jupyter Notebooks (10 mins) * Deployment Options

* Binder Project

Introduction to Apache Spark (5 mins)

* Spark Engine

* Spark SQL & DataFrames

Data Analysis Process 101 (10 mins)

We need data! (Mordor Project) (5 mins) * Download Datasets

* Raw Data -> DataFrame

A few data analysis techniques: (1 hour) * filter

* transform

* correlate

* visualize

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DAY1 KEYNOTE: The Trust Talks

When: Friday, Aug 7, 09:30 - 10:45 PDT

Where: BioHacking Vlg

Speakers: Nina Alli, Vee Schmitt, Yusuf Henriques, Josh O'Connor, Cannibal, Devabhaktuni Srikrishna, Najla Lindsay, Nate DeNicola

SpeakerBio: Nina Alli
No BIO available

SpeakerBio: Vee Schmitt
Patient, Hacker

SpeakerBio: Yusuf Henriques
Army Veteran, Entrepreneur

SpeakerBio: Josh O'Connor
Recording Producer, Future Social Worker

SpeakerBio: Cannibal
Hacker, Maker

SpeakerBio: Devabhaktuni Srikrishna
Data Scientist

SpeakerBio: Najla Lindsay
DFIR Scientist, BHV Speaker Ops

SpeakerBio: Nate DeNicola , MD
Telehealth, Physician

Description:

Nina Alli, Executive Director of the Biohacking Village, interviews folks in the biomedical and health industry for their insight and thoughts on where healthcare is and calls to action. They were not informed of the questions, these are real reactions and real talk.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DAY2 KEYNOTE: Understanding DIYBio and Community Labs - A Social Science Approach

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: BioHacking Vlg

SpeakerBio: Yong-Bee

Yong-Bee is a doctoral candidate at George Mason's Biodefense program. He studies how biotechnology and society are expanding the population of those participating in the life sciences. He loves to go for hikes, travel outside the US, play video games, and strike up conversations with random people.

Description:

The Do-It-Yourself Biology (DIYBio) community arose starting in the mid-2000's. This community falls is typically described in two ways in public discourse. More conservative elements paint this community as a cause of concern - increased access to life sciences technology, knowledge, and capabilities raises concerns that community members may produce biological products for harmful purposes. More progressive elements highlight that the self-enforcing nature of the community mitigates harmful outcomes, and that the DIYBio community can also contribute to society by addressing gaps in science education, innovation, and workforce training.

This presentation will be a distillation of work I have been doing during my PhD work to build a better understanding of community labs - one of several significant segments of the DIYBio community. I will provide a risk assessment framework that national security experts appear to use in assessing risks from emerging technologies and related phenomena. I will then describe how this risk assessment framework may interpret DIYBio as an emerging threat to national security. The remainder of the presentation will be on presenting the nuances that complicate this allegedly straightforward assessment.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DAY3 KEYNOTE: Why is Security Hard?

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: BioHacking Vlg

SpeakerBio: Seth Carmody , PhD

Seth Carmody, PhD is the Vice President of Regulatory Strategy at MedCrypt. Prior to MedCrypt, Dr. Carmody worked as the cybersecurity program manager at the U.S. FDA's Center for Devices. Carmody brings eight years of experience in guiding medical device technology policy.

Description:

Security debt, the byproduct of market incentives, creates risk for healthcare stakeholders. The manifestation of that risk into harm and the resulting impact do not necessarily change active market incentives. As result, there is a series of cascading failures in the development, regulation, and maintenance of healthcare technology. Therefore, to make a significant impact on the security posture of healthcare and medical devices in particular, a system of policy and technological solutions must; align with active market incentives, enhance the effect of latent market incentives, or create new market incentives. A comprehensive solution is explored.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DDSAT-1

When: Friday, Aug 7, 12:00 - 17:59 PDT

Where: Aerospace VIg Workshop

Description:

If CPX SimpleSat was, well, too simple, try your hand at hacking DDSat-1. Here you'll get to experiment with RF exploitation by attacking a mock satellite over RF while it is talking to a mock ground station. You'll be able to mimic the style of RF commands being generated as a part of Hack-a-Sat, but in a more simplified and user friendly manner.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DDSAT-1

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

If CPX SimpleSat was, well, too simple, try your hand at hacking DDSat-1. Here you'll get to experiment with RF exploitation by attacking a mock satellite over RF while it is talking to a mock ground station. You'll be able to mimic the style of RF commands being generated as a part of Hack-a-Sat, but in a more simplified and user friendly manner.

[Return to Index](#) - Add to  - ics [Calendar](#) file

AEV - Sunday - 09:00-13:59 PDT

Title: DDSAT-1

When: Sunday, Aug 9, 09:00 - 13:59 PDT

Where: Aerospace VIg Workshop

Description:

If CPX SimpleSat was, well, too simple, try your hand at hacking DDSat-1. Here you'll get to experiment with RF exploitation by attacking a mock satellite over RF while it is talking to a mock ground station. You'll be able to mimic the style of RF commands being generated as a part of Hack-a-Sat, but in a more simplified and user friendly manner.

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Saturday - 15:00-15:30 PDT

Title: Decentralization in a Centralized world

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: Monero Vlg

SpeakerBio:rehr

No BIO available

Description:No Description available

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Saturday - 11:00-11:59 PDT

Title: Decentralized Finance (DeFi) - ready for prime time ?

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: Blockchain Vlg

SpeakerBio:Ryan Rubin

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Deep Dive into Adversary Emulation - Ransomware Edition

When: Thursday, Aug 6, 14:15 - 15:15 PDT

Where: Red Team VIg

SpeakerBio:Jorge Orchilles

Jorge Orchilles is the Chief Technology Officer of SCYTHE and co-creator of the C2 Matrix project. He led the offensive security team at Citi for over 10 years; a SANS Certified Instructor; author of Security 564: Red Team Exercises and Adversary Emulation; founding member of MITRE Engenuity Center of Threat-Informed Defense; CVSSv3.1 working group voting member; co-author of a Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry; ISSA Fellow; and NSI Technologist Fellow. Jorge holds post-graduate degrees from Stanford and Florida International University in Advanced Computer Security & Master of Science.

Description:

A day hardly goes by without hearing about another ransomware attack. This talk will focus on how to emulate a ransomware attack without introducing risk. We will understand how ransomware works, learn how criminals are evolving to get paid, create an adversary emulation plan that is safe but valuable for enterprises, and discuss how to defend against ransomware attacks.

Adversary Emulation is a type of ethical hacking engagement where the Red Team emulates how an adversary operates, leveraging the same tactics, techniques, and procedures (TTPs), against a target organization. The goal of these engagements is to train and improve people, process, and technology. This is in contrast to a penetration test that focuses on testing technology and preventive controls. Adversary emulations are performed using a structured approach following industry methodologies and frameworks (such as MITRE ATT&CK) and leverage Cyber Threat Intelligence to emulate a malicious actor that has the opportunity, intent, and capability to attack the target organization. Adversary Emulations may be performed in a blind manner (Red Team Engagement) or non-blind (Purple Team) with the Blue Team having full knowledge of the engagement.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Deep Space Networking

When: Friday, Aug 7, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

Deep space communications utilize TCP/IP protocols with some added assistance from a TCP Convergence Layer and the Bundle Protocol. In this workshop, participants will examine the store-and-forward techniques used to transmit "bundles" of information from one host to another via a relay system. Using the latest version of Wireshark, participants will examine the TCP Convergence Header and locate the first packet of a bundle and the first and second legs of the relay process, as reassembled by Wireshark. After identifying the content contained within the bundle, participants will create a filter to locate the last packet of a bundle and examine key fields of the Bundle Protocol, including fields that define priority, destination type, endpoint IDs, and reporting of bundle delivery.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Deep Space Networking

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

Deep space communications utilize TCP/IP protocols with some added assistance from a TCP Convergence Layer and the Bundle Protocol. In this workshop, participants will examine the store-and-forward techniques used to transmit "bundles" of information from one host to another via a relay system. Using the latest version of Wireshark, participants will examine the TCP Convergence Header and locate the first packet of a bundle and the first and second legs of the relay process, as reassembled by Wireshark. After identifying the content contained within the bundle, participants will create a filter to locate the last packet of a bundle and examine key fields of the Bundle Protocol, including fields that define priority, destination type, endpoint IDs, and reporting of bundle delivery.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Deep Space Networking

When: Sunday, Aug 9, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

Deep space communications utilize TCP/IP protocols with some added assistance from a TCP Convergence Layer and the Bundle Protocol. In this workshop, participants will examine the store-and-forward techniques used to transmit "bundles" of information from one host to another via a relay system. Using the latest version of Wireshark, participants will examine the TCP Convergence Header and locate the first packet of a bundle and the first and second legs of the relay process, as reassembled by Wireshark. After identifying the content contained within the bundle, participants will create a filter to locate the last packet of a bundle and examine key fields of the Bundle Protocol, including fields that define priority, destination type, endpoint IDs, and reporting of bundle delivery.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DEF CON Groups Panel

When: Sunday, Aug 9, 15:00 - 15:59 PDT

Where: DEF CON Groups

Speakers:Brent White / B1TK1LL3R,Casey Bourbonnais / ADAM_915,Jayson E. Street,April C Wright

SpeakerBio:Brent White / B1TK1LL3R

Brent is a Sr. Security Consultant at NTT Security as well as a Trusted Advisor for the Tennessee Department of Safety and Homeland Security on the topics of Physical and Cyber Security. He is also the founder of the Nashville DEF CON group (DC615), and is the Global Coordinator for the DEF CON conference “Groups” program. He has held the role of Web/Project Manager and IT Security Director for a global franchise company as well as Web Manager and information security positions for multiple television personalities and television shows on The Travel Channel.

Twitter: [@brentwdesign](#)

SpeakerBio:Casey Bourbonnais / ADAM_915

No BIO available

Twitter: [@Bourbonnais_c](#)

SpeakerBio:Jayson E. Street

Jayson E. Street is the VP of InfoSec at SphereNY ... He is also DEF CON Groups Global Ambassador. Jayson battled a dragon during the Fire Run in Barcelona Spain. He 'accidentally broke into a shark tank in the Dominican Republic and climbed the pyramid of Giza (until the guards carrying AK-47s expressed their displeasure). He consulted with the Secret Service in 2007 on the WIFI security of the White House, and has had tea with a Lebanese General in Beirut. Jayson never finished High School but does have his GED. His first book is used as course material at four colleges in three countries (that he knows of), and he has spoken at numerous universities in the US and gave an eight-hour lecture at the Beijing Institute of Technology in 2014. Outside of standardized education, Jayson has spoken numerous times at DEF CON, at the first six DerbyCons and at many other Cons (Hack in Paris, Nuit Du Hack, IT-Defense, SYSCAN360, PH-Neutral, etc....) around the world. He was also on the David Letterman show (seriously) though he is still waiting for Stephen Colbert to have him on his show! Jayson is only one degree away from Kevin Bacon after awkward hugging Oliver Stone and Jimmy Fallon. He started in security and law enforcement over 30 years ago and has always striven to make things more secure. Jayson has been in the Information Security industry for over 18 years, and once broke into a high scale hotel in the South of France - barefoot - wearing Teenage Mutant Ninja Turtles pajamas. He was also noted as the best janitor of all McDonald's in the South East Texas region for 2 consecutive years.

SpeakerBio:April C Wright

April C. Wright is a hacker, author, teacher, and community leader who has been breaking, making, fixing, and defending the security of global critical communications and connections for over 25 years. She is an international speaker and trainer, educating and advising on matters of privacy and information security with the goal of safeguarding the digital components we rely on every day. April has held roles on defensive, operational, adversarial, and development teams throughout her career and is currently a Senior Application Security Architect. Her book, “Fixing An Insecure Software Life Cycle” was published through O’Reilly, and she is currently writing a new book to be published by No Starch Press. She is a co-host for the SecurityWeekly family of webcasts. April has spoken and contributed to numerous worldwide security conferences (often during repeat appearances), including BlackHat on three continents, DEF CON on two continents, DerbyCon, GRRcon, Layer 8, Hack in Paris, DefCamp Romania, ITWeb South Africa. She has also presented for the US Government and industry organizations such as OWASP and ISSA. She has started multiple small businesses including a non-profit and a photography studio. April currently handles communications for the Official DEF CON Groups global community outreach, and in 2017 she co-founded the local Boston meetup “DC617”. April has collected dozens of certifications to add capital letters at the end of her name, almost died in Dracula’s secret staircase, and once read on The Onion that researchers at the University of North Carolina released a comprehensive report in 2014 confirming her status as the “most significant and interesting person currently inhabiting the earth”, and it was on ‘teh internet’ so it must be true.

Twitter: [@aprilwright](#)

Description:

Do you love DEF CON? Do you hate having to wait for it all year? Well, thanks to DEF CON groups, you're able to carry the spirit of DEF CON with you year round, and with local people, transcending borders, languages, and anything else that may separate us! In this moderated panel, your DEF CON groups team who works behind the scenes to make DCG possible will discuss what DCG is all about, getting involved in the community, starting your own local group, and Q&A.

Twitch: <https://www.twitch.tv/jaysonstreet>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DEF CON Scavenger Hunt

When: Friday, Aug 7, 10:00 - 19:59 PDT

Where: See Description or Village

Description:

While everyone in the world finds themselves socially distanced and in some level of quarantine, we are bringing the DEF CON Scavenger Hunt to you. As this year is so different, teams will be limited to one person.

The list will drop at 10AM on Friday, with items to produce and tasks to accomplish until the game ends at noon on Sunday. You will be competing for glory, bragging rights, and prizes (that you can pick up at the table, during the next in-person DEF CON).

Forum: <https://forum.defcon.org/node/232938>

Discord: <https://discord.com/channels/708208267699945503/711049278163779605>

Twitter: <https://twitter.com/DefConScavHunt>

Web: <http://defconscavhunt.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DEF CON Scavenger Hunt

When: Saturday, Aug 8, 10:00 - 19:59 PDT

Where: See Description or Village

Description:

While everyone in the world finds themselves socially distanced and in some level of quarantine, we are bringing the DEF CON Scavenger Hunt to you. As this year is so different, teams will be limited to one person.

The list will drop at 10AM on Friday, with items to produce and tasks to accomplish until the game ends at noon on Sunday. You will be competing for glory, bragging rights, and prizes (that you can pick up at the table, during the next in-person DEF CON).

Forum: <https://forum.defcon.org/node/232938>

Discord: <https://discord.com/channels/708208267699945503/711049278163779605>

Twitter: <https://twitter.com/DefConScavHunt>

Web: <http://defconscavhunt.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DEF CON Scavenger Hunt

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: See Description or Village

Description:

While everyone in the world finds themselves socially distanced and in some level of quarantine, we are bringing the DEF CON Scavenger Hunt to you. As this year is so different, teams will be limited to one person.

The list will drop at 10AM on Friday, with items to produce and tasks to accomplish until the game ends at noon on Sunday. You will be competing for glory, bragging rights, and prizes (that you can pick up at the table, during the next in-person DEF CON).

Forum: <https://forum.defcon.org/node/232938>

Discord: <https://discord.com/channels/708208267699945503/711049278163779605>

Twitter: <https://twitter.com/DefConScavHunt>

Web: <http://defconscavhunt.com/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defcon Ham Radio Fox Hunting Contest

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

In the world of amateur radio, groups of hams will often put together a transmitter hunt (also called "fox hunting") in order to hone their radio direction finding skills to locate one or more hidden radio transmitters broadcasting. The Defcon Fox Hunt will require participants to locate a number of hidden radio transmitters broadcasting at very low power which are hidden throughout the conference. Each transmitter will provide a clue or one time use ticket which will prove the player found the fox transmitter. A map with rough search areas will be given to participants to guide them on their hunt. Additional hints and tips will be provided throughout Defcon at the contest table to help people who find themselves stuck. A small prize to be determined will be given to each participant who locates all of the foxes each day. In previous years a custom made embroidered velcro-backed patch was given out or a "fun" trophy. The patches are always a big hit so it's likely we'll do that again this year if selected.

Forum: <https://forum.defcon.org/node/232947>

Discord: <https://discord.com/channels/708208267699945503/711645275902574633>

Twitter: <https://twitter.com/richsentme>

Web: <https://defcon27foxhunt.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defcon Ham Radio Fox Hunting Contest

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

In the world of amateur radio, groups of hams will often put together a transmitter hunt (also called "fox hunting") in order to hone their radio direction finding skills to locate one or more hidden radio transmitters broadcasting. The Defcon Fox Hunt will require participants to locate a number of hidden radio transmitters broadcasting at very low power which are hidden throughout the conference. Each transmitter will provide a clue or one time use ticket which will prove the player found the fox transmitter. A map with rough search areas will be given to participants to guide them on their hunt. Additional hints and tips will be provided throughout Defcon at the contest table to help people who find themselves stuck. A small prize to be determined will be given to each participant who locates all of the foxes each day. In previous years a custom made embroidered velcro-backed patch was given out or a "fun" trophy. The patches are always a big hit so it's likely we'll do that again this year if selected.

Forum: <https://forum.defcon.org/node/232947>

Discord: <https://discord.com/channels/708208267699945503/711645275902574633>

Twitter: <https://twitter.com/richsentme>

Web: <https://defcon27foxhunt.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defcon Ham Radio Fox Hunting Contest

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

In the world of amateur radio, groups of hams will often put together a transmitter hunt (also called "fox hunting") in order to hone their radio direction finding skills to locate one or more hidden radio transmitters broadcasting. The Defcon Fox Hunt will require participants to locate a number of hidden radio transmitters broadcasting at very low power which are hidden throughout the conference. Each transmitter will provide a clue or one time use ticket which will prove the player found the fox transmitter. A map with rough search areas will be given to participants to guide them on their hunt. Additional hints and tips will be provided throughout Defcon at the contest table to help people who find themselves stuck. A small prize to be determined will be given to each participant who locates all of the foxes each day. In previous years a custom made embroidered velcro-backed patch was given out or a "fun" trophy. The patches are always a big hit so it's likely we'll do that again this year if selected.

Forum: <https://forum.defcon.org/node/232947>

Discord: <https://discord.com/channels/708208267699945503/711645275902574633>

Twitter: <https://twitter.com/richsentme>

Web: <https://defcon27foxhunt.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Defending Your UNIX Hosts (Intermediate)

When: Saturday, Aug 8, 15:30 - 16:15 PDT

Where: Blue Team Vlg - Workshop Track 1

Speakers: Daniel Ward, Samuel Gasparro

SpeakerBio: Daniel Ward

Information Security / Linux Systems Engineer, based in Strasbourg, France.

My background is comprised largely of Linux Systems Administration, Architecture & Engineering, data recovery / incident response.

Twitter: [@ghostinthecable](https://twitter.com/ghostinthecable)

SpeakerBio: Samuel Gasparro

No BIO available

Description:

Over the past 7 months, I have created an open-source monitoring suite called Secsuite. Secsuite is a fully automated Threat Detection, System Monitorization / Notifier suite for UNIX Sysadmins & Users alike. Secsuite has multiple packages, the focus in this workshop shall be Inframon, which is able to monitor, defend & notify you about your infrastructure, probing your hosts for:

- Apache Server Status
- Bandwidth Usage
- CPU Load Averages & Temperatures
- Disk Space Usage
- Latency time
- Memory (RAM) Usage
- Users Monitor

Over the past 7 months, I have created an open-source monitoring suite called Secsuite. Secsuite is a fully automated Threat Detection, System Monitorization / Notifier suite for UNIX Sysadmins & Users alike. Secsuite has multiple packages, the focus in this workshop shall be Inframon, which is able to monitor, defend & notify you about your infrastructure, probing your hosts for:

- Apache Server Status
- Bandwidth Usage
- CPU Load Averages & Temperatures
- Disk Space Usage
- Latency time
- Memory (RAM) Usage
- Users Monitor

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Demystifying Modern Windows Rootkits

When: Thursday, Aug 6, 15:30 - 15:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Bill Demirkapi , Independent Security Researcher

Bill is a student at the Rochester Institute of Technology with an intense passion for Windows Internals. Bill's interests include game hacking, reverse engineering malware, and exploit development. In his pursuit to make the world a better place, Bill constantly looks for the next big vulnerability following the motto "break anything and everything".

Twitter: [@BillDemirkapi](#)

Description:

This talk will demystify the process of writing a rootkit, moving past theory and instead walking the audience through the process of going from a driver that says "Hello World" to a driver that abuses never-before-seen hooking methods to control the user-mode network stack. Analysis includes common patterns seen in malware and the drawbacks that come with malware in kernel-mode rather than user-mode. We'll walk through writing a rootkit from scratch, discussing how to load a rootkit, how to communicate with a rootkit, and how to hide a rootkit. With every method, we'll look into the drawbacks ranging from usability to detection vectors. The best part? We'll do this all under the radar, evading PatchGuard and anti-virus.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

[#track-1-live](#): <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Deploying Pi-hole: More Than an Ad Blocker (Beginner)

When: Sunday, Aug 9, 12:00 - 13:30 PDT

Where: Blue Team Vlg - Workshop Track 1

SpeakerBio: Ben Hughes

Ben Hughes (@CyberPraesidium) brings over 15 years of diverse experience in cyber security, IT, and law. He leads Polito's commercial services including pen testing, DFIR, and threat hunting. Prior to joining Polito, Ben worked on APT hunt teams at federal and commercial clients. He holds CISSP, GWAPT, and GCFA certifications.

Twitter: [@CyberPraesidium](#)

Description:

Pi-hole is a popular open source DNS server that can block ads network-wide, before they even reach your browser. As it effectively functions as a DNS sinkhole, Pi-hole can be configured to securely handle DNS requests for your network devices and automatically block not just ads, but a variety of malicious traffic. This workshop will walk you through how to quickly deploy Pi-hole to protect your home network or in a lab environment. A Raspberry Pi is optional; a Docker container, lightweight virtual machine, or even an old computer will work just fine.

This hands-on workshop will cover the following training outline: * Intro to Pi-hole

* Main features and latest features in the brand new 5.0 release * Deployment options * Network design and DNS/DHCP considerations * HA/failover considerations

* Initial install and configuration

* Using blacklists and whitelists

* Viewing metrics and logs

* What's next? Advanced features and possibilities

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Detecting Fake 4G Base Stations in Real Time

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Cooper Quintin , Senior Staff Technologist, EFF

Cooper is a security researcher and Senior Staff Technologist with the EFF threat lab. He has worked on projects such as Privacy Badger and Canary Watch. With his colleagues at threat lab he has helped discover state sponsored malware and nation state actors such as Dark Caracal and Operation Manul. He has also performed security trainings for activists, non profit workers and ordinary folks around the world. He also was a co-founder of the Hackbloc hacktivist collective and published several issues of the DIY hacker zine "Hack This Zine." In his spare time he enjoys playing music and playing with his kid and imagining a better future.

Description:

4G based IMSI catchers such as the Hailstorm are becoming more popular with governments and law enforcement around the world, as well as spies, and even criminals. Until now IMSI catcher detection has focused on 2G IMSI catchers such as the Stingray which are quickly falling out of favor. In this talk we will tell you how 4G IMSI Catchers might work to the best of our knowledge, and what they can and can't do. We demonstrate a brand new software project to detect fake 4G base stations, with open source software and relatively cheap hardware. And finally we will present a comprehensive plan to dramatically limit the capabilities of IMSI catchers (with the long term goal of making them useless once and for all).

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Sunday - 09:00-09:30 PDT

Title: Detecting hand-crafted social engineering emails with a bleeding-edge neural language model

When: Sunday, Aug 9, 09:00 - 09:30 PDT

Where: AI Vlg

Speakers: Younghoo Lee, Joshua Saxe

SpeakerBio: Younghoo Lee

No BIO available

SpeakerBio: Joshua Saxe

No BIO available

Description: No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Detecting The Not-PowerShell Gang (Intermediate)

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio: Mangatas Tondang

Professionally, Mangatas is a Threat Hunter for one of the major Canadian Telecommunication company. As a blue teamer, he is passionate on learning and breaking the hacking tools to pieces and try to develop detection against them. He also love following and building detection from the recent intelligence report on different APT groups. Coming from a school that taught him broad spectrum of Information Security, he also love exploring application security, reverse engineering, and script tools that can help him and his coworkers. He wouldn't be here without community support, that's why he love to give security training for other people and currently he is also a member of CTF challenge development team for his almatamater. Outside the Security world, He is a guitarist and also "wannabe" astrophotographer.

Twitter: [@tas_kmanager](https://twitter.com/tas_kmanager)

Description:

Since the advancement of security features released in PowerShell version 5, Red Team folks are forced to not use PowerShell to have successful and undetectable engagements. Some of them even push the boundary and created their own Not-PowerShell tools and released it to the public. As a Blue Teamer, this means we need to reinforce our perimeter against these tools. This talk will uncover some of the popular Not-PowerShell tools followed by how the blue teams can still spot these tools and build detection on it.

This talk will look into several not-powershell tools and craft several detection tactics based on their mechanism. We will utilize common logging tools, Sysmon and Windows Logs (Integrated to SIEM).

We will start with Introduction and will quickly go through the common mechanism used by the not-powershell tools

Tools we are going to look at are:

- InvisiShell
- NoPowerShell
- PowerShdll
- PowerLessShell
- And some other tools with similar mechanism

After getting familiar with the mechanisms, we will put our blue hat back and see what artifacts left by these tools and build reliable detection for each mechanisms leaving small room for false positives. At the end of the day, the blue team will be awarded with some queries (also known as rules or use cases) that they can use and deploy at their own SIEM solution.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Differential Privacy..more important than ever in the world of Covid-19

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio:Aditi Joshi

Aditi Joshi works in Google Cloud's Security and Privacy Engineering team. Before Google, she was focused on data privacy research especially in health care with a focus on user trust at the core. She joined Google because she was excited about the work that Google was doing in privacy on a massive scale. She believes that privacy is a human right and will continue to work towards that end.

Description:

The goal of this talk is to explain the concept of anonymization and differential privacy, as well as offer up Codelabs and modules with the purpose of explaining Google's open source Differential Privacy library and other tools for implementation purposes. We will offer up our Covid Mobility reports as a case study and talk about the importance of privacy preserving aggregation from a social science perspective.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Digital Health Technologies in the NIH All of Us Research Program

When: Friday, Aug 7, 14:00 - 14:30 PDT

Where: BioHacking Vlg

SpeakerBio:Michelle Holko , PhD, PMP

Michelle Holko, PhD, PMP, is a White House Presidential Innovation Fellow working with NIH's All of Us Research Program. Her technical expertise is in genomics and bioinformatics, and her work lies at the intersection of health and health security, technology, data/analytics, and biosecurity policy.

Description:

The National Institutes of Health's (NIH) All of Us Research Program (AoURP) aims to enroll at least one million US participants from diverse backgrounds; collect electronic health record (EHR) data, survey data, physical measurements, biospecimens for genomics and other assays, and digital health data; and create a researcher database and tools to enable precision medicine research. Since inception, digital health technologies (DHT) have been envisioned as integral to achieving the goals of the program. A "bring your own device (BYOD) pilot for collecting Fitbit data from participants' devices was developed with more recent integration of Apple HealthKit data donation and additional DHTs planned in the future. This presentation will describe 1) the initial process to assess, curate, and include Fitbit BYOD data in the All of Us Researcher Workbench, 2) the diversity and assessment of under-represented in biomedical research (UBR) in Fitbit BYOD participants compared with overall AoU participant population, and 3) future DHT studies planned for AoURP.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Discovering Cloud File Storage Artifacts

When: Saturday, Aug 8, 15:30 - 17:30 PDT

Where: Cloud Vlg

SpeakerBio: Michael Wylie , Director of Cybersecurity Services, Richey May Technology Solution
Michael Wylie (Twitter: @TheMikeWylie), MBA, CISSP is the Director of Cybersecurity Services at Richey May Technology Solutions. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, cloud security, penetration tests, risk management, and training. Michael has developed and taught numerous courses for the U.S. Department of Defense, DEFCON, Universities, and for clients around the world. Michael is the winner of numerous SANS challenge coins and holds the following credentials: CISSP, CCNA R&S, CCNA CyberOps, GMON, GPEN, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, Security+, Project+, and more.
Twitter: @TheMikeWylie

Description:

Organizational data is rapidly moving to the cloud, but it's not always intentional. The shift from on-premise data storage to the cloud constitutes a significant challenge and risk to the modern enterprise. The use of cloud file storage applications is on the rise for both consumer and business systems, which results in interesting data and metadata sitting on endpoints. In this talk, we'll examine the large footprints of popular cloud file storage applications such as OneDrive and Box - learning what information can be enumerated from each cloud file storage solution. In some scenarios, data can be carved out from cache, restoring sensitive documents no longer on an endpoint.

Attendees will:

- Understand why it's critical to investigate cloud file storage applications during an incident
- Learn what files are available to examiners during an incident (e.g. local, cloud, deleted, and cached)
- See what kind of cloud file storage user activity can be audited
- Be introduced to two scenarios of unauthorized data transfer to investigate
- Be introduced to where and how different cloud file storage applications log
- Learn how to examine incidents with suspected data exfiltration using corporate issued and person cloud file storage use

The slides and labs will take a deep dive into Microsoft OneDrive, Google Drive, Dropbox, Box, and Citrix ShareFile to first understand what is known about the applications and artifacts left behind, then move into hands-on labs to analyze registry keys, log files, and other traces left behind by the applications.

YouTube: https://www.youtube.com/watch?v=gwBG_oKDINQ

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

Return to Index - Add to  - ics [Calendar](#) file

Title: Discovering ELK The First Time - Lessons Learned Over 2 Years (Beginner)

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio: TheDrPinky

Dr. Pinky has been a computer scientist for the US Air Force for the last six years. She specializes in threat hunting and digital forensics for both Linux and Windows operating systems. You can find DrPinky in the infosec area as the social media coordinator for BSides San Antonio, participating in the San Antonio Hackers Association (SAHA), and presenting at events such as SANS Blue Team Summit and Texas Cyber Summit.

Twitter: [@TheDrPinky](https://twitter.com/TheDrPinky)

Description:

ELK has become one of the favorite tools of blue teamers across the world. However, when you're first getting used to ELK, you may be overwhelmed and not fully understanding what is happening. There is more to do with it than simply feed in logs and search it in a pretty web UI! This talk will focus on things I wish I knew about ELK back when I was first learning it to help provide some quick wins for those new to ELK, and maybe a few tidbits for those who already use it.

Elastic, Logstash, and Kibana (ELK) continue to keep becoming more popular with blue teamers - there's plenty of documentation, you can custom develop anything you want with it due to the fact it's open source, and it's free! However, those first starting out with ELK can become quickly overwhelmed. When these people finally get the hang of ELK, they still may be missing some critical understanding that limits them - why can't I filter by hostname? What do these pretty yellow triangles really mean? This is because most people will get used to just Kibana - not rest of the stack. In this talk I'll cover lessons I wish I learned a lot sooner about ELK that would have helped me out - and hopefully they help you too!

Lesson 1: Elastic and Kibana are NOT the same. Going into the differences, why they get confused, and what the actual differences are.

Lesson 2: Logstash is more powerful than you give it credit for, but is incredibly overwhelming. Here's some ways to get some quick bang for buck.

Lesson 3: How do you go about feeding in your own custom documents to ELK? This will quickly go into popular ways to feed logs into ELK, and if that doesn't help, how to feed in other information to ELK through a more manual approach. Never know when a custom script output would be better put in elastic!

Lesson 4: Don't forget about your Linux logs! With Linux we may be more used to relying on rsyslog to forward everything - but this most likely just captures your application logs. What about the equivalency of event logs on Linux? This will (very) briefly introduce auditd, how to forward it to ELK, and how to best parse through it.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Discovering Hidden Properties to Attack Node.js ecosystem

When: Thursday, Aug 6, 09:30 - 09:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Feng Xiao , security researcher at Georgia Tech

Feng Xiao is a security researcher at Georgia Tech. His research interests include software/system security. He has published three papers on top security venues such as DEFCON, IEEE S&P, and CCS.

<https://fxiao.me/>

Description:

Node.js is widely used for developing both server-side and desktop applications. It provides a cross-platform execution environment for JavaScript programs. Due to the increasing popularity, the security of Node.js is critical to web servers and desktop clients.

We present a novel attack method against the Node.js platform, called hidden property abusing (HPA). The new attack leverages the widely-used data exchanging feature of JavaScript to tamper critical program states of Node.js programs, like server-side applications. HPA entitles remote attackers to launch serious attacks, such as stealing confidential data, bypassing security checks, and launching denial of service attacks. To help developers detect the HPA issues of their Node.js applications, we develop a tool, named LYNX, that utilizes hybrid program analysis to automatically reveal HPA vulnerabilities and even synthesize exploits. We apply LYNX on a set of widely-used Node.js programs and identify 13 previously unknown vulnerabilities. LYNX successfully generates 10 severe exploits. We have reported all of our findings to the Node.js community. At the time of paper writing, we have received the confirmation of 12 vulnerabilities and got 12 CVEs assigned. Moreover, we collaborated with an authoritative public vulnerability database to help them use a new vulnerability notion and description in related security issues.

The talk consists of four parts. First, we will introduce recent offensive research on Node.js. Second, we will introduce HPA by demonstrating an exploit on a widely-used web framework. Third, we will explain how to leverage program analysis techniques to automatically detect and exploit HPA. In the end, we will have a comprehensive evaluation which discusses how we identified 13 HPA 0days with the help of our detection method.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Saturday - 11:30-12:30 PDT

Title: Discussion: What makes a good ham radio operator?

When: Saturday, Aug 8, 11:30 - 12:30 PDT

Where: Ham Radio Vlg

Description:

Panel discussion around what makes a good ham operator, as opposed to a 'lid' (a bad operator). We'll also talk about all of the strange lingo ham radio loves to use.

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Dissecting Wireless Privacy In Aviation

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: Aerospace VIg

SpeakerBio: Martin Strohmeier

Martin Strohmeier is a Junior Research Fellow of Kellogg College, University of Oxford and a Senior Scientist at the Swiss Cyber Defence Campus. The main focus of his work has been the design, implementation, and analysis of security protocols for cyber-physical systems, specifically those used in critical infrastructures such as aviation (civil and military). Using these domains as a driver for the real-world applicability of his research, his work has been published in many diverse venues, spanning wireless communications, cryptography, systems security, sensor networking, privacy, and aviation.

After his DPhil, he has been extending his interests towards areas of open-source intelligence, privacy issues in aviation and satellite environments, and most recently adversarial machine learning. Martin is also a co-founder of the aviation research network OpenSky where he is responsible for communication and research activities.

Description:

A multitude of wireless technologies are used within air traffic communication. From a conceptual perspective, all of them are insecure as confidentiality was never part of their design and they could not keep up with the change in threat models. This talk analyzes the current state of wireless privacy in aviation, covering air traffic control and datalink communication. We show how combining publicly available data sources enables global tracking of every aircraft for anyone interested. In particular, we present various case studies to demonstrate how anyone can undermine the privacy of military, governmental and corporate operators. Finally, we look at some industry responses and illustrate the futility of the current attempts to maintain privacy for aircraft owners in a world of ubiquitous sensor surveillance.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DIY Diabetics and a Million Boluses

When: Saturday, Aug 8, 15:15 - 15:59 PDT

Where: BioHacking Vlg

Speakers:Dr. Mike Rushanan,Julian Suleder

SpeakerBio:Dr. Mike Rushanan

Dr. Mike Rushanan is the Director of Medical Security at Harbor Labs and is a security expert in diabetes management. Dr. Rushanan received his PhD in Computer Science through the Johns Hopkins University Health and Medical Security Lab studying under Dr. Avi Rubin.

SpeakerBio:Julian Suleder

Julian Suleder is a Security Analyst & Researcher at ERNW Research GmbH in Heidelberg, Germany. His research interest is the security of medical devices as he holds a master's degree in medical informatics from Heidelberg University and Heilbronn University, Germany.

Description:No Description available

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Dj St3rling

When: Saturday, Aug 8, 20:00 - 20:59 PDT

Where: See Description or Village

Description:

Performing for his second year in a row at DEF CON, Dj St3rling loves to spin electronic music. When he's not making music, he enjoys: bowling, eating tacos, sleeping, and CTF!

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Facebook: <https://www.facebook.com/OfficialDjSt3rling>

Soundcloud: <https://soundcloud.com/theycallmest3r>

Instagram: <https://www.instagram.com/theycallmest3r/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCG - Saturday - 15:15-15:59 PDT

Title: DNS New World Order, version 1.4: QuadX! DoH! DoT! Da Fuq?

When: Saturday, Aug 8, 15:15 - 15:59 PDT

Where: DEF CON Groups

Description:

Presentation by DC603 (New Hampshire, USA)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: DNS Privacy

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Matt Cheung

Matt developed his interest and skills in cryptography during graduate work in Mathematics and Computer Science. During this time he had an internship at HRL Laboratories LLC working on implementing elliptic curve support for a Secure (in the honest-but-curious model) Two-Party Computation protocol. From there he implemented the version secure in the malicious model. He currently works as an Application Security Consultant at Veracode, but continues to learn about cryptography in his spare time.

Description:

While there are many protocols such as https that encrypt network sessions to preserve the security and privacy of that communication, typically the first step is a DNS query. DNS, being a plaintext protocol, can compromise the privacy of a user. In this talk we will discuss what can be currently done and potential future protocols such as Oblivious DNS.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DNSSECTION: A practical attack on DNSSEC Zone Walking

When: Thursday, Aug 6, 11:30 - 11:59 PDT

Where: DEF CON Q&A Twitch

Speakers:Hadrien Barral,Rémi Géraud-Stewart

SpeakerBio:Hadrien Barral , Hacker

Hadrien Barral is an R&D engineer, focusing on security and high-assurance software. He enjoys hacking on exotic hardware.

SpeakerBio:Rémi Géraud-Stewart , Hacker

Rémi Géraud-Stewart is a cryptologist and security expert with École Normale Supérieure in Paris, focusing on intrusion and cyberwarfare.

Description:

Domain Name System (DNS) is an ubiquitous and essential component of the Internet. It performs translations between identifiers and resources (mostly domain names and computers, but not only), yet remains often invisible to the user. But DNS is not harmless: although not intended to be a general purpose database, it has been extended to incorporate additional types of information. Including information that should not be there.

In this talk we show how to exploit DNSSEC zone walking to perform advanced recon operations, on a real case, namely to obtain client private information from a large European cloud provider. This constitutes the first practical zone walking attack at such a scale.

Using this exploit we collected a substantial amount of private information, enough to share some interesting statistics. By the end of this talk, you will have everything you need to know to perform similar attacks -- and resist them.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Domain Fronting is Dead, Long Live Domain Fronting: Using TLS 1.3 to evade censors, bypass network defenses, and blend in with the noise

When: Thursday, Aug 6, 16:30 - 16:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Erik Hunstad , CTO, SIXGEN

Erik Hunstad is a security expert and researcher who realized the power of programming and security when he coded an algorithm to reduce the search space of possible Master Lock combinations in RAPTOR. Erik is the CTO and Adversary Emulation Lead at SIXGEN where he specializes in deploying the latest offensive security techniques against customers. He previously worked for the Department of Defense.

Twitter: [@SixGenInc](#)

Description:

Domain fronting, the technique of circumventing internet censorship and monitoring by obfuscating the domain of an HTTPS connection was killed by major cloud providers in April of 2018. However, with the arrival of TLS 1.3, new technologies enable a new kind of domain fronting. This time, network monitoring and internet censorship tools are able to be fooled on multiple levels. This talk will give an overview of what domain fronting is, how it used to work, how TLS 1.3 enables a new form of domain fronting, and what it looks like to network monitoring. You can circumvent censorship and monitoring today without modifying your tools using an open source TCP and UDP pluggable transport tool that will be released alongside this talk.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Don't Be Silly - It's Only a Lightbulb

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Eyal Itkin , Vulnerability Researcher at Check Point Software Technologies

Eyal Itkin is a vulnerability researcher in the Malware and Vulnerability Research group at Check Point Software Technologies. Eyal has an extensive background in security research, that includes years of experience in embedded network devices and protocols, bug bounties from all popular interpreter languages, and an award by Microsoft for his CFG enhancement white paper. When not breaking RDP or FAX, he loves bouldering, swimming, and thinking about the next target for his research.

Twitter: [@Eyalltkin](https://twitter.com/Eyalltkin)

Description:

A few years ago, a team of academic researchers showed how they can take over and control smart lightbulbs, and how this in turn allows them to create a chain reaction that can spread throughout a modern city. Their research brought up an interesting question: aside from triggering a blackout (and maybe a few epilepsy seizures), could these lightbulbs pose a serious risk to our network security? Could attackers somehow bridge the gap between the physical IoT network (the lightbulbs) and even more appealing targets, such as the computer network in our homes, offices or even our smart cities?

We're here to tell you the answer is: Yes.

Join us as we take a deep dive into the world of ZigBee IoT devices. Continuing from where the previous research left off, we go right to the core: the smart hub that acts as a bridge between the IP network and the ZigBee network. And let me tell you this, this harsh embedded environment is surely not on our side. With a maximal message size of less than 128 bytes, complex state machines and various strict timing constraints, this challenge is going to be tough.

After a long journey, we finally made it. By masquerading as a legitimate ZigBee lightbulb, we were able to exploit vulnerabilities we found in the bridge, which enabled us to infiltrate the lucrative IP network using a remote over-the-air ZigBee exploit.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](https://discord.com/channels/708208267699945503/733079621402099732)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Don't Ruck Us Again - The Exploit Returns

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio:Gal Zror , Research team leader in Aleph Research

Gal Zror is a research team leader in Aleph Research group at HCL AppScan, based in Herzliya Israel. Gal has extensive experience with vulnerability research and specialized in embedded systems and protocols. Gal is also an amateur boxer and a tiki culture enthusiast.

Twitter: [@waveburst](https://twitter.com/waveburst)

Description:

From the researchers who brought to you "Don't Ruck Us Too Hard" comes a brand new follow-up research. This summer! We will show that all of Ruckus Wireless "ZoneDirector" and the ""Unleashed"" devices are still vulnerable.

This follow-up research includes six new vulnerabilities, such as command injection, information leakage, credentials overwrite, and stack overflow and XSS. With these vulnerabilities, we were able to achieve two new and different pre-auth RCEs. Combined with the first research, that is five entirely different RCEs in total. We also found that Ruckus did not fix some of the vulnerabilities from the first research correctly, and they are still exploitable by using a very neat payload :).

Other cool stuff about this research:

We will share a new Ghidra script we used to map the critical sections in the webserver binary that were later found vulnerable. We managed to fingerprinted Universities and Organizations that were vulnerable from the internet. BlackHat uses Ruckus Wireless for Wi-Fi solutions.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](https://discord.com/channels/708208267699945503/733079621402099732)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Don't Go Postal Over Mail In Voting

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: Voting Vlg

SpeakerBio: Bianca Lewis , Founder and CEO, Girls Who Hack; Secure OpenVote

No BIO available

Description:

As the previous DEF CON Voting Villages have proved, our voting equipment and infrastructure are very vulnerable to multiple types of attacks. But now, with everything that's going on in the world ,voting by mail is the new vulnerable thing! Instead of focusing on problems and broken things, this talk will focus on simple fixes that vendors and governments can put into action right now. Starting with the registering to vote, then moving through parts of the entire system, BiaSciLab will offer suggestions on how simple practices and changes in thinking can improve the security of the entire system.

Last year, in the Voting Village BiaSciLab did a talk on the election systems problems and howto fix them. This year with voting by mail, new problems are appearing! Like States not allowing people to vote by mail! Breaking down these flaws and offering real solutions for each one, BiaSciLab will bring hope in the face of this daunting and complex security problem in these hard times.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

Return to Index - Add to  - ics [Calendar](#) file

LPV - Friday - 15:00-15:30 PDT

Title: Doors, Cameras, and Mantraps OH MY!

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: Lockpick Vlg

SpeakerBio:Dylan The Magician

No BIO available

Description:

Lockpicking, door bypassing, and physical security are among the more eye catching components of an on premises risk assessment. It always draws the most questions and gets the most staff popping over to see what's going on. I suppose it's because the physical space is personal, it isn't digital and hence it draws more focus. I do on premises risk assessment and I want to tell you a bit about how the process goes with my company and share my personal philosophies on how I do my engagements. What I hope to gain is a stronger focus on Physical Security, or PhysSec, in the Cybersecurity domain.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

Return to Index - Add to  - ics [Calendar](#) file

Title: Dos, Donts and How-Tos of crypto building blocks using Java

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Crypto & Privacy VIg

SpeakerBio: Mansi Sheth

Mansi Sheth is a Principal Security Researcher at Veracode Inc. In her career, she has been involved with breaking, defending and building secure applications. Mansi researches various languages and technologies, finds insecure usage in customer code and suggests automation measures in finding vulnerabilities for Veracode's Binary Static Analysis service. She is an avid traveller with the motto "If not now, then when?"

Description:

Do you feel unequipped to understand real world crypto attacks? Are you overwhelmed with the over-abundance of choices provided by any modern cryptography API, to make a secure decision while choosing a randomness provider, encryption scheme or digital signature APIs? Are you on top of all the latest happenings in cryptographic communities, to know which cryptographic primitives is deemed broken? Due to sheer lack of documentation of the chosen API, do you feel paralyzed on where and how to start designing or analyzing any cryptographic systems?

If any of these answers are "yes", come join me in this talk. I will be going over each cryptographic primitive like Random Number Generators, Encryption/Decryption algorithms, message authentication codes, digital signatures, password storage etc pointing out dos and donts based on evaluating bunch of leading cryptographic implementations. Java being one of the most widely used enterprise language, and simultaneously one of the most chaotic cryptography architecture, we chose it to get into some live coding exercises to showcase its secure usage, while also future-proofing your cryptographic applications.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Friday - 13:30-13:59 PDT

Title: Double Spending in BSV, is it Possible?

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: Blockchain Vlg

SpeakerBio:Poming Lee

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: DragonOS - How I kept busy during COVID19

When: Thursday, Aug 6, 09:00 - 09:01 PDT

Where: Wireless Vlg

SpeakerBio:cemaxecuter

I'd rather keep my job experience private. I am from a small town, but have been all over. I've met the developers of OpenWRT in Germany, developed my own line of dual mesh radios under the AWDMESH name, back when OpenMesh used the OM1P's, put together the ZoneMinder DVD using remastersys, and now fast forward I've put all my effort during COVID19 into making the Linux distributions called DragonOS 10, DragonOS LTS, and DragonOS Focal specifically for SDRs.

I've easily put hundreds and hundreds of hours into testing and making everything work along with making videos for YouTube in the hopes they'll help others develop a passion for Linux and SDRs.

A buddy of mine by the name of Rick from Wireless Village encouraged me to talk about DragonOS 10/LTS and now my latest work, DragonOS Focal.

Description:

Intro

Why I started DragonOS

What is DragonOS

What problems and challenges I had to overcome What companies and developers helped and who donated equipment

This talk is available on YouTube.

Talk: <https://www.youtube.com/watch?v=69k1Dmr2Ruk>

Return to Index - Add to  - ics [Calendar](#) file

Title: Drinks with Recruiters

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: Career Hacking Vlg

Speakers:Kris Rides,Rachel Bozeman,Matt Duren,Pete Radloff

SpeakerBio:Kris Rides

No BIO available

SpeakerBio:Rachel Bozeman

No BIO available

SpeakerBio:Matt Duren

No BIO available

SpeakerBio:Pete Radloff

No BIO available

Description:

Recruiters are people too, but given the backlashes we have seen along with the poor spam messages from "recruiters" you would think otherwise. So a group of recruiters familiar with the community will sit down over drinks and share some of their horror stories. From this you will learn how to improve your job search, your interviewing and maybe come to enjoy working with recruiters.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Dumpster Fires: 6 Things About IR I Learned by Being a Firefighter

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Packet Hacking VIg - Talk

SpeakerBio:Dr. Catherine Ullman , Sr. Information Security Forensic Analyst

Dr. Catherine J. Ullman (Twitter: @investigatorchi) is a security researcher, speaker, and Senior Information Security Forensic Analyst at University at Buffalo with over 20 years of highly technical experience. In her current role, Cathy is a data 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 amongst faculty and staff via a comprehensive department-wide program 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 prestigious information security conferences including DEF CON and Hacker Halted. 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.

Twitter: [@investigatorchi](https://twitter.com/investigatorchi)

Description:

Threats surround us like a ring of burning fire. Unfortunately, incident response doesn't come naturally to an operational mindset where the focus tends to be on reactive problem solving. As a volunteer firefighter for over twenty years, investigatorchi has learned a lot about what is and isn't effective. There are surprising parallels between fighting real-life fires and the fire-fighting that passes for today's incident response. For example, striking a balance between swift response and patient reflection is often the difference between life and death, in a very literal sense for the firefighter and a figurative sense for the security professional. It's also all too easy to get tunnel vision and focus on the wrong areas, costing precious time. The security world is full of dumpster fires these days, so join this session to learn from a good firefighter what makes a good security person.

YouTube: <http://youtube.com/wallofsheep>

Twitch: <http://twitch.tv/wallofsheep>

Facebook: <http://facebook.com/wallofsheep/>

Periscope: <https://t.co/gnl7JLlftA?amp=1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: EFF Tech Trivia Pub Quiz

When: Friday, Aug 7, 17:00 - 18:59 PDT

Where: See Description or Village

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 Plaque and EFF swag pack. The second and third place teams will also win great EFF gear.

Forum: <https://forum.defcon.org/node/232941>

Discord: <https://discord.com/channels/708208267699945503/711644552573747350>

Twitter: <https://twitter.com/EFF>

Web: <https://eff.org>

[Return to Index](#) - Add to  - ics [Calendar](#) file

POV - Friday - 15:30-16:30 PDT

Title: Election Security

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: See Description or Village

Description:

This event requires registration. Please see the below URL for details.

Registration: <https://www.eventbrite.com/e/def-con-community-roundtable-election-security-tickets-115977739541>

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Saturday - 14:30-14:59 PDT

Title: Electronic Ballot Return Standards & Guidelines

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: Voting Vlg

Speakers:Forrest Senti,Mattie Gullixson

SpeakerBio:Forrest Senti , Director of Business & Government Affairs, National Cybersecurity Center

No BIO available

SpeakerBio:Mattie Gullixson , Secure the Vote Project Manager, National Cybersecurity Center

No BIO available

Description:

The emergence of new electronic ballot return methods creates an opportunity for greater vote access and potential enfranchisement, but also raises concerns about security in an increasingly tumultuous cyber-election landscape. The challenge of security is further compounded by a lack of proactive guidance from the federal level on developing these new technologies, leaving a gap in the secure development of the technologies to adopt an elections framework and approach to security. Experts from the National Cybersecurity Center (NCC) will offer a draft of security guidelines for the new electronic ballot return platforms to consider, and for federal agencies to adopt. The guidelines format mimics the Voluntary Voting System Guidelines created by the Election Assistance Commission.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Emulating an Adversary with Imperfect Intelligence

When: Saturday, Aug 8, 17:45 - 18:45 PDT

Where: Red Team Vlg

SpeakerBio: Adam Pennington

Adam Pennington (@_whatshisface) leads ATT&CK at The MITRE Corporation and collected much of the intelligence leveraged in creating ATT&CK's initial techniques. He has spent much of his 11 years with MITRE studying and preaching the use of deception for intelligence gathering. Prior to joining MITRE, Adam was a researcher at Carnegie Mellon's Parallel Data Lab and earned his BS and MS degrees in Computer Science and Electrical and Computer Engineering as well as the 2017 Alumni Service Award from Carnegie Mellon University. Adam has presented and published in a number of venues including FIRST CTI, USENIX Security and ACM Transactions on Information and System Security.

Twitter: @ _whatshisface

Description:

Adversary emulation has become an increasingly common type of engagement where red teams look to known threat groups to inspire the actions and behaviors used. While scoping activity might make operating easier, emulation introduces a new set of challenges to planning. How do you know how an adversary behaves? What do you do if you only know part of the picture? How do you turn all of that into a plan? In this talk I'll examine how we can start building an adversary profile from the open source intel in MITRE ATT&CK. Open source intel often doesn't give a complete picture of an adversary, and I'll talk about some of where these gaps come from, how to spot them, and some ways of filling them in. I'll work through a process for turning the profile we've created into an adversary emulation plan expressed in ATT&CK and how we can stay aligned with that plan as we operate.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Entrepreneurial Adventures: What It Takes to Start A Company

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Career Hacking Vlg

SpeakerBio: Bryson Bort

Founder of SCYTHE, next generation attack emulation platform; GRIMM, cybersecurity consultancy; ICS Village Co-Founder, 501c3 for ICS security awareness. Senior Fellow for Cyber/National Security at R Street and National Security Institute; Advisor to the Army Cyber Institute and DHS/CISA.

Description:

So you're not crazy, you just want to start your own company. Which kinda takes a level of crazy to pull it off. We'll talk through what it takes to be an entrepreneur, ideation and the phases of startup, different kinds of companies (service, product, non-profit), how and why (or why not) to raise capital, types of investors, legal requirements, working (or not) with friends, challenges, building total/service addressable market size, back-office administration, employee benefits, equity, pricing, Intellectual Property Rights, economics, and resources for more information and networking. Will include anecdotes and insights my experiences starting several companies and from multiple Founders across the spectrum.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Enumerating Cloud File Storage Gems

When: Friday, Aug 7, 16:45 - 17:45 PDT

Where: Red Team Vlg

SpeakerBio: Michael Wylie , Director of Cybersecurity Services, Richey May Technology Solution
Michael Wylie (Twitter: @TheMikeWylie), MBA, CISSP is the Director of Cybersecurity Services at Richey May Technology Solutions. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, cloud security, penetration tests, risk management, and training. Michael has developed and taught numerous courses for the U.S. Department of Defense, DEFCON, Universities, and for clients around the world. Michael is the winner of numerous SANS challenge coins and holds the following credentials: CISSP, CCNA R&S, CCNA CyberOps, GMON, GPEN, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, Security+, Project+, and more.

Twitter: @TheMikeWylie

Description:

Organizational data is rapidly moving to the cloud, but it's not always intentional. The shift from on-premise data storage to the cloud constitutes a significant challenge and risk to the modern enterprise. The use of cloud file storage applications is on the rise for both consumer and business systems, which results in interesting data and metadata sitting on endpoints. In this talk, we'll examine the large footprints of popular cloud file storage applications such as OneDrive and Box - learning what information can be enumerated from each cloud file storage solution. In some scenarios, data can be carved out from cache, restoring sensitive documents no longer on an endpoint.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Friday - 23:00-23:59 PDT

Title: ERPwnage - a red team approach to targeting SAP

When: Friday, Aug 7, 23:00 - 23:59 PDT

Where: Red Team VIg

SpeakerBio: Austin Marck

No BIO available

Description:

The crown jewels are ripe for the taking. ERP systems like SAP are being targeted more than ever and red teams need the tools to demonstrate these threats. We'll demonstrate the TTPs needed to emulate real threats with lateral movement techniques in, out, and between SAP systems.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: European regulatory trends for Artificial Intelligence: same impact on US as GDPR?

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Julia Reinhardt

Julia is based in San Francisco and works as a tech policy consultant and privacy professional. As a Mozilla Fellow in Residence, she assesses opportunities and limitations of European approaches on Trustworthy AI in Silicon Valley and their potential for US businesses and advocacy.

In her first career as a German diplomat, she worked, among others, in EU negotiations on GDPR and on doing outreach and communicating for Germany in the Western US. Inspired by the Silicon Valley tech and policy network she built over the years and her understanding of EU policy-making, she has been consulting tech companies and non-profits in the Bay Area on European tech regulation for four years now. She holds an M.A. in International Relations from Sciences Po Paris, an M.A. in European Studies from Universität Osnabrück, and completed graduate and postgraduate coursework at UC Berkeley, American University of Beirut and Stanford University.

Description:

My paper focuses on how the European Ethics Guidelines for Trustworthy AI will be implemented – whether directly or indirectly and if at all – in Silicon Valley. My perspective incorporates also other related EU regulation that affects AI, in particular the GDPR and the deriving obligation to implement the principles of “privacy by design” and “privacy by default” (Art. 25 GDPR).

During my Mozilla Fellowship (April 2020 through April 2021), I work on finding out what impact the new European Ethics Guidelines for Trustworthy AI will have on US businesses, how useful they find these, as well as how they’re evaluated by activists, and whether we therefore will see a similar trend with them as we saw with the GDPR. I want to share with DEFCON Privacy Village an insight into my research and what this means for Silicon Valley positions on future EU regulation.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Thursday - 11:45-12:45 PDT

Title: Evil Genius: Why you shouldn't trust that keyboard

When: Thursday, Aug 6, 11:45 - 12:45 PDT

Where: Red Team VIg

Speakers:Farith Perez, Mauro Cáseres

SpeakerBio:Farith Perez

No BIO available

SpeakerBio:Mauro Cáseres

Mauro Cáseres (@mauroeldritch) is an argentine hacker and speaker. He spoke at DEF CON 26 Las Vegas (Recon & Data Duplication Villages), DevFest Siberia, DragonJAR Colombia, Roadsec Brasil, and DC7831 Nizhny Novgorod. Currently working as SecOps for the Argentine Ministry of Production.

Twitter: [@mauroeldritch](https://twitter.com/mauroeldritch)

Description:No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Evil Printer: How to Hack Windows Machines with Printing Protocol

When: Sunday, Aug 9, 09:30 - 09:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Chuanda Ding, Zhipeng Huo

SpeakerBio: Chuanda Ding , Senior Researcher, Tencent Security Xuanwu Lab

Chuanda Ding is a senior security researcher on Windows platform security. He leads EcoSec team at Tencent Security Xuanwu Lab. He was a speaker at Black Hat Europe 2018, DEF CON China 2018, CanSecWest 2017, CanSecWest 2016, and QCon Beijing 2016.

Twitter: [@FlowerCode_](#)

SpeakerBio: Zhipeng Huo , Senior Researcher, Tencent Security Xuanwu Lab

Zhipeng Huo is a senior security researcher on Windows and macOS platform security at Tencent Security Xuanwu Lab. He reported Microsoft Edge sandbox escape bugs in 2017, 2018, and 2020. He was a speaker at Black Hat Europe 2018.

Twitter: [@R3dF09](#)

Description:

Printer Spooler service, one of the important services in Microsoft Windows, has existed for more than 25 years. It runs at highest privilege level, unsandboxed, does networking, and dynamically loads third-party binaries. What could possibly go wrong?

In this talk, we will walk you through an incredibly fun bug we have discovered in printer spooler service. It can be exploited both locally and remotely, escapes sandbox, executes arbitrary code, and also elevates to SYSTEM. While Microsoft managed to develop the most restrictive sandbox for Microsoft Edge, this bug easily goes through it like it's a sieve.

We will talk in detail the implementation of this ancient service, the method we used to discover and exploit the bug, and also throw in some tips and tricks for logic bugs in between.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Executing Red Team Scenarios with Built-in Scenario Place

When: Saturday, Aug 8, 03:30 - 04:30 PDT

Where: Red Team VIg

Speakers:Erdener Uyan,Gökberk Gülğün

SpeakerBio:Erdener Uyan

Erdener Uyan has worked in the field of information security for over 10 years as an engineer, researcher, practitioner and educator. His wide-ranging career has spanned many areas of information security, including research and development of very high-assurance, multi-level secure systems for use in government and the military, research and development of cryptographic systems, and general IT security and compliance for commercial organizations in the industries. Uyan earned his PhD degree in Cryptography at the Middle East Technical University.

SpeakerBio:Gökberk Gülğün

Gökberk Gülğün has worked in the field of information security for over 6 years as an engineer, researcher, practitioner and educator. Currently, Offensive security engineer at an industry-leading bank based in the Turkey. Plans and conducts full-scope Red Team engagements that simulate realistic, targeted, attacks. Responsible for performing host infrastructure penetration testing, physical security assessments, web and mobile application testing, social engineering engagements, source code reviews, embedded device assessments, and wireless penetration tests. In the past, he has given several presentations on Malware Analysis, Red Team Operations, discovered Odays and IoT security.

Description:

Red Team activities are undoubtedly one of the fastest developing solutions against the cyber attacks of today. In this talk, we'll take a look at our work on an open-source proactive machine learning powered automation tool that performs red team simulations. This automation tool provides the opportunity to try out all available attack scenarios, thereby helping the community, especially organizations, to develop mechanisms to protect against these attacks before attackers do. Currently, red, blue and purple teams are improving day by day with the contributions made by open source. We will demonstrate the scenario playbook developed to collect the scenarios prepared for the red, blue and purple team on a single scenario place. The aim of this playbook is to protect the systems from such attack vectors, to examine the attack scenarios, to protect their systems by viewing the protection mechanisms and to contribute to these scenarios. With the built-in Scenario Place, people can either run these scenarios or check the scenario configurations on their systems. All scenario titles are prepared in accordance with MITRE and Cyber Kill Chain. All scenarios from various teams such as Atomic Red Team, Mitre and TIBER-EU are fed into the application as input.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Experimental Aviation, Risks And Rewards

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Aerospace Vlg

SpeakerBio: Patrick Kiley , Principal Security Consultant, Rapid7

Patrick Kiley (GXPN, GPEN, GAWN, GCIH, CISSP, MCSE) has over 18 years of information security experience working with both private sector employers and the Department of Energy/National Nuclear Security Administration (NNSA). While he was with the NNSA he built the NNSA's SOC and spent several years working for emergency teams. Patrick has performed research in Avionics security and Internet connected transportation platforms. Patrick has experience in all aspects of penetration testing, security engineering, hardware hacking, IoT, Autonomous Vehicles and CAN bus.

Twitter: [@gigstorm](https://twitter.com/gigstorm)

Description:

This talk will cover a hacker's perspective of building your own aircraft, what I consider to be the ultimate maker/hacker project. Over 10 years ago, I decided to see if I could build an aircraft from a set of plans. The model I chose was a 4 seat AeroCanard FG, a somewhat controversial derivative of the Cozy Mark IV. The Cozy itself was also a derivative, basically a widened version of the Burt Rutan designed Long EZ. This talk will cover why someone would choose to build their own aircraft. All of these topics will cover the risk as I see it as a professional who has been in the information risk field his entire professional career.

- I will break this talk down into the following topics.
- FAA and the 51% rule
- Plans vs Kits
- Composite vs riveted aluminum construction
- Making changes to tested designs
- Engine selection, aviation engines vs conversions
- Avionics selection

I will complete the talk with some discussion around becoming a test pilot, what you will become when you finally fly your creation.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

Return to Index - Add to  - ics [Calendar](#) file

BCV - Sunday - 12:00-12:40 PDT

Title: exploit insecure crypto wallet

When: Sunday, Aug 9, 12:00 - 12:40 PDT

Where: Blockchain Vlg

Speakers:Minzhi He,peiyu wang

SpeakerBio:Minzhi He

No BIO available

SpeakerBio:peiyu wang

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Exploiting Key Space Vulnerabilities in the Physical World

When: Friday, Aug 7, 16:30 - 16:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Bill Graydon , Principal, Research, GGR Security

Bill Graydon is a principal researcher 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 DEF CON's Lock Bypass Village. He's received various degrees in computer engineering, security, and forensics and comes from a broad background of work experience in cyber security, software development, anti-money laundering, and infectious disease detection.

Description:

Imagine being able to get together with a few of your co-workers, look at your office keys and derive a building master key. Or you may not have any working key at all: you could impression the lock, or use one of the many ways we'll present in this talk to put together little bits of information from a lock to create a working key.

We apply information theory - the concept behind the "entropy" of a password - in an easy to understand way to show how every little bit of information about a system can be used to defeat it. The audience will be able to pull any key out of their pocket and understand how it works and how an attacker can create it covertly, and open whatever lock it is for, or even a lock it isn't for, that shares the same system.

We'll explain how to produce either a single final key, or a set small enough to economically brute force - and release a software tool to let anyone quickly try out all possibilities in an easy-to-visualize way.

Finally, we will discuss possible solutions to these problems and introduce vulnerabilities our research has uncovered in high-security systems like Medeco, Abloy, and Mul-T-Lock - including releasing a set of only 159 possible top level master key codes for certain large Medeco mastered systems.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Exploiting Spacecraft

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: Aerospace Vlg

SpeakerBio: Brandon Bailey

Brandon Bailey is a cybersecurity senior project leader at The Aerospace Corporation. He has more than 14 years of experience supporting the intelligence and civil space arena. Bailey's specialties include vulnerability assessments/ penetration testing for space systems and infusing secure coding principles within the software supply chain. Before joining Aerospace, Bailey worked for NASA, where he was responsible for building and maintaining a software testing and research laboratory to include a robust cybersecurity range as well as spearheading innovative cybersecurity assessments of ground infrastructure that support NASA's mission operations. While at NASA, Bailey was honored with several group and individual awards, including NASA's Exceptional Service Medal for his landmark cybersecurity work, NASA's Early Career Achievement Award, and NASA Agency Honor Awards for Information Assurance/Cybersecurity. He has also contributed to teams who have received honorable mention in the 2012 and 2016 NASA's Software of the Year competition. Bailey graduated summa cum laude with a bachelor's degree in electrical engineering from West Virginia University and currently holds multiple certifications in the cybersecurity field. He recently co-authored Aerospace's Center for Space Policy and Strategy's Defending Spacecraft in the Cyber Domain paper which outlines security principles that can be applied on-board the spacecraft to improve its security posture.

Description:

This presentation will describe the high-level cyber threat landscape for space systems and focus on three examples: Command Replay Attack, Command Link Intrusion, and Denial of Service using GPS jamming. These three attacks were performed using high fidelity ground-to-space simulators to demonstrate the benefit of performing such research using simulation. These simulations leverage many of the same software components used in operations today for several operational missions. Recommendations are provided on how to protect against the attacks and references are provided so the audience can build their own simulations to begin their own research.

This event will be coordinated on the DEF CON Discord server, in channel #av-space-text.

Discord: <https://discord.com/channels/708208267699945503/732394328105943180>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Exploring vulnerabilities in Smart Sex Toys, the exciting side of IoT research

When: Friday, Aug 7, 12:15 - 12:59 PDT

Where: IOT VIg

SpeakerBio:Denise Giusto Bilic

Denise Giusto Bilic is an Information Systems Engineer graduated from the National Technological University of Argentina. Nowadays she specializes in mobile and IoT security.

Denise currently works as a Security Researcher at ESET, where part of her job is preparing technical and educational materials related to information security. She has participated as a speaker in many international security conferences. She is also a co-organizer of NotPinkCon Security Conference.

Description:

Smart sex toys are a huge topic – and we’re not talking about their size! The Internet of Things (IoT) has triggered many personal items to become connected and smart, watches, toothbrushes, glasses and even toilets, to name just a few. The adult toy market has not been left behind with new models of toys that include the opportunity to connect them to the Internet and allow them to be remotely controlled.

IoT devices and their vulnerabilities are frequently discussed in the media, and sex toys are not the exception. Many of them have holes in them. Keep focused, we mean holes and bugs in the software. This is despite the sensitivity of the extremely personal information they handle. We analyzed the security of the Android applications that control the most frequently purchased models of connected sexual pleasure devices, to determine the extent to which the confidentiality of user data could be vulnerable. Our research revealed interesting security flaws derived from both the implementation of the application and the design of the device, affecting the storage and processing of information.

If you’re one of the many users who have a smart sex toy connected to the internet, or plan to buy one, you cannot miss this talk, it may have you shaking in your seat. Our presentation may make you reconsider connecting it ever again or not purchasing one at all.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Sunday - 13:00-13:59 PDT

Title: Faults in our Pi Stars: Security Issues and Challenges in Deep Reinforcement Learning

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: AI Vlg

SpeakerBio: Vahid Behzadan

No BIO available

Description: No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PAYV - Friday - 11:00-11:59 PDT

Title: Fear and Loathing in Payment Bug Bounty

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Payment Vlg

SpeakerBio: Timur Yunusov

No BIO available

Description:

Bug bounty - is an easy-to-start-and-succeed Information Security area. Low entry barriers, money engagement, low risks of being sued. But none of these can be applied when it comes to payment vulnerabilities. It's hard to find banks which allow digging into their assets. We're here to try and change it! Start with payment security today, vulnerabilities are waiting.

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

Return to Index - Add to  - ics [Calendar](#) file

Title: Fear, Uncertainty, and Doubt about Human Microchip Implants

When: Sunday, Aug 9, 11:00 - 11:30 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Zhanna Malekos Smith

No BIO available

Description:

Why are some U.S. lawmakers calling for a preemptive ban on human microchip implants? Today, more than 50,000 people worldwide have elected to receive microchip implants. This technology is especially popular in Sweden, where more than 4,000 Swedes are replacing keycards for chip implants to use for gym access, e-tickets on railway travel, and even store emergency contact information and social media profiles. While chip implants are gradually being embraced, some U.S. lawmakers are taking preemptive action to prohibit forced microchipping and calling it “a rabbit hole I don’t think we should go down”. Together, let’s go down this ‘rabbit hole’ to explore the legal, technical, and ethical implications of human microchipping.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ETV - Friday - 10:00-10:59 PDT

Title: Federal Communications Commission

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Ethics VIg

SpeakerBio:Comm. Geoffrey Starks
No BIO available

Description:

This will be a pre-recorded talk.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Federal Trade Commission

When: Saturday, Aug 8, 14:10 - 15:20 PDT

Where: Ethics VIg

SpeakerBio:Comm. Rohit Chopra

No BIO available

Description:

This will be a 40-minute pre-recorded talk, followed by a 30-minute live Q&A session.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Fighting a Virus with a Spreadsheet (Beginner)

When: Friday, Aug 7, 18:30 - 18:59 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio: Allen Baranov

Allen is a seasoned information security professional with over 15 years of experience in diverse industry verticals such as banking and finance, manufacturing, retail and communications. He has extensive knowledge of IT Security Management, Compliance including ISO 27001 and PCI DSS, Network Security Architecture Review, Vulnerability assessment and Security Architecture.

As a senior information security consultant (GRC) at Sense of Security, Allen brings a keen interest in IT risk assessments and risk treatment, security architecture and design, PCI-DSS gap assessments, security strategy and roadmaps as well as the creation of frameworks, policies, standards and procedures.

Supported by his Bachelor of Commerce and multiple industry-recognised certifications such as PCI QSA, CISSP, and SABSA, Allen has extensive experience across many security compliance implementations and security operation requirements. His strengths include understanding the technical intricacies of security and the need for a balanced approach to meet business objectives and addressing risks appropriately.

Twitter: [@abaranov](https://twitter.com/abaranov)

Description:

On 27 June 2017, a piece of malware raced across the globe and took out many organisations including some that were similar to the one I was employed at. But we were safe and, in fact, not worried at all.

All thanks to clever use of spreadsheets.

In this talk, given entirely within Excel (yes, really) I go through the methods used to protect the organisation from this malware. If a talk given entirely in Excel sounds boring - you haven't seen this talk.

I have (virtually) given this talk twice - at a local Australian conference called ComfyCon and at a charity event hosted by Second Order Chaos. In both cases - they were blown away by the creativity of the "slides" and the fun way that this is presented.

There is a serious aspect to this though. It goes through the different phases of getting an effective patch program established. It has a 'hacker' aspect to it in that it asks people to be excited and interested and curious about their security controls and the processes that lead to the outcomes that are achieved.

I've thrown some humour and some easter eggs into the presentation.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: File Encryption For Actual Humans

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: Crypto & Privacy Vlg

SpeakerBio:David Kane-Parry

dkp has been breaking and building the software you depend on for decades. Presently, at Spotify. Previously, security lead for login.gov and other projects at 18F, cryptography policy owner at Amazon, and hacker-for-hire just about everywhere else.

Description:

I wrote a proof-of-concept tool to demonstrate that, by combining modern cryptography and human-centered design, emailing encrypted files doesn't have to be so thoroughly insecure. Better than Signal? No, but for many, emailing password-protected zip files is the only user-accessible and/or policy-approved method at their disposal. Leaving them at the mercy of broken algorithms and broken approaches to password selection. But both of which can fixed in about 100 lines of Python.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Film Festival: Project Immerse: A Deepfake Paranoid Thriller

When: Saturday, Aug 8, 13:00 - 14:30 PDT

Where: See Description or Village

Description:

From the creators of "Frankenstein AI" and "Sherlock Holmes and the Internet of Things" comes a new experiment AI manipulation... Co-created with AI, Project immerse is a paranoid thriller set in a world of deepfakes, shallow fakes, and bots...

Project Immerse leads up to 100 participants through a tangled conspiracy-driven collaborative investigation, co-created with AI. Running time: 80 minutes

The first 100 participants in the Zoom waiting room will be admitted.

Zoom: <https://columbiauniversity.zoom.us/j/99339173670>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Film Festival: Project Immerse: A Deepfake Paranoid Thriller

When: Saturday, Aug 8, 18:30 - 19:59 PDT

Where: See Description or Village

Description:

From the creators of "Frankenstein AI" and "Sherlock Holmes and the Internet of Things" comes a new experiment AI manipulation... Co-created with AI, Project immerse is a paranoid thriller set in a world of deepfakes, shallow fakes, and bots...

Project Immerse leads up to 100 participants through a tangled conspiracy-driven collaborative investigation, co-created with AI. Running time: 80 minutes

The first 100 participants in the Zoom waiting room will be admitted.

Zoom: <https://columbiauniversity.zoom.us/j/96118316158>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Finding and Exploiting Bugs in Multiplayer Game Engines

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Jack Baker

Jack Baker is a professional reverse engineer and amateur video game hacker. Jack is most known for having the same name as a Resident Evil villain.

Description:

Unreal Engine 4 and Unity3D dominate the multiplayer gaming landscape. They're also complicated pieces of software written in C and C++. In this talk, Jack will share the results of months of bug hunting in multiplayer game networking protocols. Be prepared for memory disclosures, speedhacks, and WONTFIX vulnerabilities.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fireside Chat with Dr. Amy Abernethy and Adama Ibrahim

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: BioHacking Vlg

Speakers: Adama Ibrahim, Amy Abernethy

SpeakerBio: Adama Ibrahim

No BIO available

SpeakerBio: Amy Abernethy

Amy P. Abernethy, M.D., Ph.D. is an oncologist and internationally recognized clinical data expert and clinical researcher. As the Principal Deputy Commissioner of Food and Drugs, Dr. Abernethy helps oversee FDA's day-to-day functioning and directs special and high-priority cross-cutting initiatives that impact the regulation of drugs, medical devices, tobacco and food. As acting Chief Information Officer, she oversees FDA's data and technical vision, and its execution. She has held multiple executive roles at Flatiron Health and was professor of medicine at Duke University School of Medicine, where she ran the Center for Learning Health Care and the Duke Cancer Care Research Program. Dr. Abernethy received her M.D. at Duke University, where she did her internal medicine residency, served as chief resident, and completed her hematology/oncology fellowship. She received her Ph.D. from Flinders University, her B.A. from the University of Pennsylvania and is boarded in palliative medicine.

Description:

Discussions around:

- Intersection of big data and patient rights - Real World Data and how to best serve patients in the digital era - Cybersecurity risk for medical devices - How FDA is working with security researchers (e.g., the FDA-led Evidence Accelerator at the FDA)

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fireside Chat: All about Section 230, the EARN IT Act, and What They Mean for Free Speech and Encryption

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: Crypto & Privacy Vlg

Speakers: Cathy Gellis, Riana Pfefferkorn

SpeakerBio: Cathy Gellis

Frustrated that people were making the law without asking her for her opinion, Cathy Gellis gave up a career as a web developer to become a lawyer so that she could help them not make it badly, especially where it came to technology. A former aspiring journalist and longtime fan of free speech her legal work includes defending the rights of Internet users and advocating for policy that protects online speech and innovation. She also writes about the policy implications of technology regulation on sites such as the Daily Beast, Law.com, and Techdirt.com, where she is a regular contributor.

SpeakerBio: Riana Pfefferkorn

Riana Pfefferkorn is the Associate Director of Surveillance and Cybersecurity at the Stanford Center for Internet and Society.

Description:

It seems like everyone's talking about Section 230 these days, and keen to change it, even without really knowing what it says and does. Or how badly most of the proposals to change it, such as the EARN IT Act bill, threaten all sorts of things we value, including encryption, privacy, security, and free speech online. Come to this crash course in Section 230 basics, followed by a fireside chat about EARN IT between two seasoned lawyers, to learn the truth about this crucial law, why these proposals are so terrible, and how you can take action to protect the Internet.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Food and Drug Administration

When: Saturday, Aug 8, 15:20 - 16:30 PDT

Where: Ethics VIg

SpeakerBio: Jessica Wilkerson

No BIO available

Description:

This will be a 40-minute pre-recorded talk, followed by a 30-minute live Q&A session.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: From Barista to Cyber Security Pro, Breaking the Entry Level Barrier

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Career Hacking VIg

SpeakerBio: Alyssa Miller

No BIO available

Description:

If you're a barista that has never worked in a tech job, how do you land a role in security? What if I told you there are skills you have that apply directly to roles in security. In this session we're going to get into some real talk about landing your first security gig. We will analyze the challenges that aspiring security professionals need to overcome in order to find their way into an entry level position. We'll look at the issues of job descriptions, certifications, degrees, and other job search related challenges. We'll analyze data from a recent primary research to better understand how education, certifications, mentoring, and other characteristics impact the job search. Finally we'll use that information to share tangible real strategies you can use to overcome those hiring obstacles.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: From Blackbox to Automotive Ransomware

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: Car Hacking VIg 001

Speakers:Nils Weiss,Enrico Pozzobon

SpeakerBio:Nils Weiss

Nils Weiss and Enrico Pozzobon are PhD students at the University of Applied Sciences in Regensburg. Both are focusing on automotive security research since more than 4 years. After an internship at Tesla Motors, Nils decided to focus on automotive security as a research field. During his bachelor and master program, he started with penetration testing of entire vehicles.

Enrico Pozzobon started with automotive security during his Erasmus semester at the University of Applied Sciences in Regensburg. He studied telecommunication engineering at the University of Padua. Since 3 years, Nils and Enrico are building up a laboratory for automotive penetration testing at the University of Applied Sciences in Regensburg. Besides penetration testing of automotive systems, both are contributing to open source penetration testing frameworks for automotive systems (Scapy).

SpeakerBio:Enrico Pozzobon

Nils Weiss and Enrico Pozzobon are PhD students at the University of Applied Sciences in Regensburg. Both are focusing on automotive security research since more than 4 years. After an internship at Tesla Motors, Nils decided to focus on automotive security as a research field. During his bachelor and master program, he started with penetration testing of entire vehicles.

Enrico Pozzobon started with automotive security during his Erasmus semester at the University of Applied Sciences in Regensburg. He studied telecommunication engineering at the University of Padua. Since 3 years, Nils and Enrico are building up a laboratory for automotive penetration testing at the University of Applied Sciences in Regensburg. Besides penetration testing of automotive systems, both are contributing to open source penetration testing frameworks for automotive systems (Scapy).

Description:

The lack of state of the art security features in many current cars can lead to devastating impacts for the vehicle owners and passengers. This talk presents the full path from the investigation of safety critical ECUs to the development of a proof of concept malware/ransomware affecting the whole car.

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUej1Q&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

Return to Index - Add to  - ics [Calendar](#) file

Title: From Discovery to Disclosure

When: Sunday, Aug 9, 04:45 - 05:45 PDT

Where: Red Team VIg

SpeakerBio: Ibad Shah

Professional Red Teamer in daylight and Security Researcher at night.

Description:

This session will discuss about journey from discovering vulnerabilities in an android application having premium features leading towards approaching relevant authorities, disclosing all of the required details and solutions. It is to be noted that the application has been downloaded by more than 1.5 million users and exploiting such vulnerabilities would have adverse affect on organization as reputational and regulatory. The talk will also focus on how security researchers can contact relevant authorities of organization more effectively and disclose such critical vulnerabilities.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar](#) file

PWDV - Friday - 22:30-22:40 PDT

Title: From Printers to Silver Tickets or Something (Rebroadcast)

When: Friday, Aug 7, 22:30 - 22:40 PDT

Where: Password Vlg

SpeakerBio: EvilMog

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 16:00-16:59 PDT

Title: From Printers to Silver Tickets or Something

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: Password Vlg

SpeakerBio: EvilMog

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fundamentals of Diagnostic Requests over CAN Bus

When: Friday, Aug 7, 12:00 - 12:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Robert Leale (CarFuCar)

Robert Leale (@carfucar) is an automotive hacker and a founding member of the Car Hacking Village. For more information please visit carhackingvillage.com/about

Twitter: [@carfucar](https://twitter.com/carfucar)

Description:

Data can be requested using CAN Network, but what data can you ask for? How do you know how to send requests? What type of requests can you send? What can data do with the data that you get back? How do you handle errors? So many questions on how to get started. We will answer the fundamentals of shaping a request and handling the response. Diagnostics are a way of communicating directly with Electronic Control Units in vehicle. UDS is a standard diagnostic protocol. We will explore how to format a UDS request and handle its response.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Fundamentals of Diagnostic Requests over CAN Bus

When: Saturday, Aug 8, 12:00 - 12:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio: Robert Leale (CarFuCar)

Robert Leale (@carfucar) is an automotive hacker and a founding member of the Car Hacking Village. For more information please visit carhackingvillage.com/about

Twitter: [@carfucar](https://twitter.com/carfucar)

Description:

Data can be requested using CAN Network, but what data can you ask for? How do you know how to send requests? What type of requests can you send? What can data do with the data that you get back? How do you handle errors? So many questions on how to get started. We will answer the fundamentals of shaping a request and handling the response. Diagnostics are a way of communicating directly with Electronic Control Units in vehicle. UDS is a standard diagnostic protocol. We will explore how to format a UDS request and handle its response.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Future Proofing Your Career

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: Career Hacking Vlg

SpeakerBio:Jenai Marinkovic

No BIO available

Description:

We have entered the 4th industrial revolution, a time marked by the interconnection of hyper-instrumented physical, biological, and digital worlds. The accompanying pace of technological development will exert profound changes in the way people live and work, impacting all disciplines, economies, and industries. Preparing the cybersecurity workforce for the changes that will reframe their careers requires insight and a vision of our possible future.

Next-generation security professionals will both leverage and work alongside purpose-based digital assistants to help navigate the explosion of data created by intelligent ecosystems. These virtual assistants will replace current knowledge management platforms/intranets, dashboards, and manage any security process that can be automated. As machine learning and cognitive solutions evolve in sophistication, security teams must re-examine how they organize work, design jobs, and plan for future growth. Let's futurecast near term technological trends and identify the concrete steps all security professionals need in the Age of the Intelligent Ecosystem and the Augmented Workforce.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

Return to Index - Add to  - ics [Calendar](#) file

Title: General Aviation (GA) Electronic Flight Bags (EFB)

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: Aerospace Vlg

SpeakerBio:David Robinson

Dave/Karit is currently part of the team at ZX Security in Wellington, New Zealand and works as a penetration tester. Since joining ZX Security Dave has presented at Defcon and Kiwicon along with other Cons and meetups. Along with aerospace, he has a keen interest in lock-picking and all things wireless.

Description:

Over the last while I have been looking at General Aviation (GA) Electronic Flight Bags (EFB). This talk will look at some of the potential security related issues I have noticed along the way. This talk will be a high level overview of the classes of problems which have been observed, opposed to focusing on particular products and individual bugs in these products. The goal here is to help an industry who is adding more connected services to their products and understanding the risks which the benefits bring.

The talk will highlight some categories of issues which have been identified. Along with information about why it is an issue, there will be information on methods to mitigating these security risks. I would like to see as an outcome from this talk people who develop EFBs taking away some of the ideas and mitigating the risk in their own products.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 22:40-23:30 PDT

Title: Getting Advanced with Hashcat (Rebroadcast)

When: Friday, Aug 7, 22:40 - 23:30 PDT

Where: Password Vlg

SpeakerBio: Password Village Staff
No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 18:00-18:59 PDT

Title: Getting Advanced with Hashcat

When: Friday, Aug 7, 18:00 - 18:59 PDT

Where: Password Vlg

SpeakerBio: Password Village Staff

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Getting Shells on z/OS with Surrogat Chains

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Jake Labelle , Security Consultant - F-Secure

Jake Labelle graduated from Southampton University with a MEng in Computer Science. He currently works at F-Secure in Basingstoke as a Security Consultant.

He discovered z/OS this year in January, and now can not stop dabbling. He has created a number of security labs in z/OS and is currently scripting everything in REXX. If he had a choice between a windows host and an emulated z/OS host on his laptop, it would not be a competition.

He is currently ecstatic that Hercules, a mainframe emulator, can be compiled for arm and ran on a Raspberry Pi. There is also an open source mainframe (<http://wotho.ethz.ch/tk4-/>). I'm probably carrying my portable open source mainframe with me right now.

<https://github.com/southamptonjake>

Description:

z/OS allows a user to submit a job as another user without a password with the surrogat class. However, z/OS systems often have hundreds of thousands of users and have been running for decades. This means that it is very likely that from a low priv user there is a surrogat chain that will give you special (z/OS' root).

RACF (z/OS' Security), does not allow users to view the security of resources to which they do not have access. This means that manually enumerating a chain required you to submit a reverse shell each time you wanted to move up the chain. This will take a long time with 200k users.

Gator (my tool), submits a batch job that will call a REXX program which will output the user's privs and the current surrogat chain of that user. It will then list all of that user's surrogat privs, and call the same batch job as before, but running as those users.

Gator also provides a macro that will generate a CATSO (similar to a meterpreter shell), for any of the users in the surrogat chain.

Gator can also be exported to a GraphVis python program, which will display the users information and chain as a network of nodes.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

Return to Index - Add to  - ics [Calendar](#) file

IOT - Friday - 10:45-11:45 PDT

Title: Getting Started – Building an IoT Hardware Hacking Lab

When: Friday, Aug 7, 10:45 - 11:45 PDT

Where: IOT Vlg

Description:

This learning session will focus on the subject of building an IoT hardware hacking lab. During this learning session various tools and technologies will be shown and discussed that are needed for physical disassembly, soldering, debugging, and analyzing. Covering the basic entry level to the more advanced lab equipment needed and used. After each learning objective we will have Q&A sessions

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 21:00-21:30 PDT

Title: Getting Started with Hashcat (Rebroadcast)

When: Friday, Aug 7, 21:00 - 21:30 PDT

Where: Password Vlg

SpeakerBio: Password Village Staff
No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 10:00-10:59 PDT

Title: Getting Started with Hashcat

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Password Vlg

SpeakerBio: Password Village Staff

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Friday - 14:30-15:30 PDT

Title: Getting started with the Intervillage badge

When: Friday, Aug 7, 14:30 - 15:30 PDT

Where: Monero Vlg

SpeakerBio:Michael Schloh von Bennewitz

No BIO available

Description:

Codenamed Bob, this year's electronic badge enjoys collaboration from several villages and is called the Intervillage Badge. <https://bob.monerodevices.com/> In this hour, we focus on ways to use the Intervillage Badge including: - Out of the box data storage with NFCTools - Onboarding procedure for your village use - Impersonating radio IDs in your environment - Backing up data from mobile applications - Playing the Rogues Village Game online - Navigating the Bob village network Continuing, we consider modification strategies to make the badge suit your personal village style, like adding a lanyard, printing a new enclosure, and disassembly strategies. We conclude by reviewing hardware hacks the badge may support as well as VNA assisted antenna tuning. For more information about this year's village badge (and many others), please visit the Monero Village office hours. View the schedule at Monerovillage.org and look for 'Badge Clinic'.

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

Return to Index - Add to  - ics [Calendar](#) file

Title: Ghosting the PACS-man: New Tools and Techniques

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: Wireless Vlg

Speakers: Iceman, Omikron

SpeakerBio: Iceman

No BIO available

SpeakerBio: Omikron

No BIO available

Description:

Do you fear the PACS-man? Do you lie awake at night atop your pile of RFID cards of unknown origin, pondering grand questions of access control? Is Wiegand a card or a data format? What is an "encrypted" credential and is it actually any more secure? Fear not, fellow explorer. Come discuss your woes with professional ghosts of access control and learn how to keep the PACS-man at bay. This livestream will provide a holistic context of modern access control and outline common design limitations that can be exploited when systems are not implemented correctly. From credentials, to readers, to door controllers and beyond, Babak Javadi and Iceman from the Red Team Alliance will share a practical understanding of what PACS looks like in the field, and how to intercept, clone, downgrade, replay, and one's way through the system.

The talk will demonstrate several new tools, exploits, and refined methods for compromising modern PACS, including:

- DoS Attacks Involving Improper Reconfiguration of Readers
- New iCLASS Standalone Modes for Proxmark3 RDV4.0
- Tech Downgrade Attacks: Techniques for compromising systems using high security credentials such as SEOS and DESFire EV1/EV2.
- Plus More Special Surprises!

Customers, integrators, and system designers will also learn more about best practices and defensive methods that can be used to defend systems and deter attackers.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Google Maps Hacks

When: Friday, Aug 7, 12:00 - 13:59 PDT

Where: Rogues Vlg

SpeakerBio: Simon Weckert

No BIO available

Description:

You've seen his Google Maps Hacks on international news just earlier this year, now come see the methodology behind his projects. Simon uses technology in the digital space to cleverly impact the physical space, all the while creating some playful mischief. Excited to welcome Simon to our village this year.

From Simon:

99 second hand smartphones are transported in a handcart to generate virtual traffic jam in Google Maps. Through this activity, it is possible to turn a green street red which has an impact in the physical world by navigating cars on another route to avoid being stuck in traffic. The presentation will give an insight of the hack. #googlemapshacks

Rogues Village activities will be streamed via Twitch.

Twitch: <https://www.twitch.tv/roguesvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCG - Saturday - 11:00-11:59 PDT

Title: Government Espionage on a School Lunch Budget

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: DEF CON Groups

Description:

Presentation by DC664 (Mexico)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: GPS Spoofing 101

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: Aerospace VIg

SpeakerBio:Harshad Sathaye

Harshad is a Ph.D. candidate at Northeastern University and a soon-to-be student pilot. He is a cyber security enthusiast with research interests around wireless systems security, specifically navigation systems and development of secure cyber-physical systems

Description:

With the advent of autonomous cyber-physical systems such as self-driving cars and unmanned aerial vehicles, the use of Global Positioning System (GPS) for positioning and navigation has become ubiquitous. In recent years we have seen a lot of GPS "incidents" which involve either denial of services or spoofing to mislead the receiver. This workshop will include the basics of GPS spoofing with a hands-on exercise and a discussion of state-of-the-art spoofing mitigation techniques

This event will be coordinated on the DEF CON Discord server, in channel #av-space-text.

Discord: <https://discord.com/channels/708208267699945503/732394328105943180>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTVT1 - Thursday - 10:15-10:59 PDT

Title: Graylog: An Introduction Into OpenSOC CTF Tools

When: Thursday, Aug 6, 10:15 - 10:59 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio:Lennart Koopmann

No BIO available

Twitter: [@_lennart](#)

Description:

Learn. Play. Do.

Every year the Blue Team Village hosts OpenSOC. A unique defense CTF meant to teach and test practical incident response skills in an environment that's as close to "the real thing" as it gets.

This year BTV wanted to do more. We know that some Blue Teamers might be unfamiliar with some of the tools used by OpenSOC. And we didn't want that to keep anyone from playing this incredible defense simulation.

So this year we are dedicating all day Thursday to demo the various OpenSOC tools, before OpenSOC starts on Friday. These are tools like Graylog, Moloch, Zeek, Osquery, and others that Blue Teamers rely on every day to defend their networks against attackers.

That means that after you LEARN the tools, you can PLAY the OpenSOC CTF, and then take that knowledge back to your own Blue Team to DO the work of defending your network.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Grey Hat SSH: SShenanigans

When: Friday, Aug 7, 14:15 - 15:15 PDT

Where: Red Team Vlg

SpeakerBio: Evan Anderson

Evan Anderson is the Director of Offense at Randori. He has over 15 years of experience in red teaming, vulnerability research and exploit development and is a founding member of the NCCDC Red Team. Prior to co-founding Randori, he worked at Kyrus Technologies supporting commercial and federal projects.

Description:

The Secure Shell (SSH) was designed to replace telnet/rsh with a secure channel over unsecured networks. SSH is a swiss army knife for red team engagements letting malicious actors accomplish a multitude of interesting tasks. Aside from providing access to run commands on remote systems SSH can be used to complete a myriad of other activities including hop network boundaries, maintain persistent access, download files, steal credentials, hide access and even configure what commands users run on login. This talk goes through details of how to configure and abuse ssh for a number of red team oriented goals from beginner too advanced.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Guerrilla Red Team: Decentralize the Adversary

When: Thursday, Aug 6, 10:30 - 11:30 PDT

Where: Red Team VIg

SpeakerBio: Christopher Cottrell

Christopher Cottrell is a security engineer and leader, focusing most of my career on offensive operations. I have built red teams, contributed to published works, open-sourced tools, and publicly discussed adversarial techniques. When I am not doing operations, I am refining long term strategy, uplifting the security community through red team mentoring programs, or learning about new adversarial techniques.

Description:

"Guerrilla Red Team is a methodology by which a company can grow security IQ, technical expertise, and security brainpower, resulting in an internal mesh network of trusted decentralized ethical hackers. The program requires minimal capital investment from the hosting red team. It achieves its primary goals through weekly group mentorship hosted during a four-hour block, once per week, during the workday. It forms a peer network in which guerrilla operators share ideas and techniques, and ultimately grow technically and professionally as a unit. Members of the program come from various technical disciplines, but not necessarily security-focused verticals. The cohort of five to six members follows a nine-week syllabus that takes them from someone with minimal red team experience to autonomous operations. Guerrilla Operators will have a regular cadence of operations, which will require deconfliction from the parent red team to only ensure there are no safety concerns with the proposed target. Expected outcomes for the nine-week cohort are as follows: Guerrilla operators are armed with the skills to continue their red team learning, as well as a support network for challenging tasks The parent red team has an expanded network of internal, trusted, ethical hackers. This strengthens idea generation for campaigns, and enables communication through the use of a shared and common technical language. Over time, the Guerrilla Red Team provides a steady flow of trained homegrown red team operators or security analysts The company itself benefits by having security-focused mindsets placed throughout technical disciplines, resulting in staff that are poised to ward off attacks by thinking like an attacker, functioning similarly to security-focused Site Reliability Engineers (SRE) Provides the company with verification that their security program and infrastructure are as robust as they say it is through the use of decentralized, independent low-tier actors attacking the network: an Offsec ChaosMonkey Provides the guerrilla operators real world, hands on experience in a career field that is hard to break into outside of the Federal pipeline "

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: H@cker Runw@y

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

For the second year, H@ck3r Runw@y is bringing together fashionistas out there. Make it SMART, LIGHT it up, OBFUSCATE something, or be GEEKY on fleek. Enter clothing, shoes, jewelry, hats or accessories. If you wear it, the runway can handle it. Predesign entry or create something on the fly. Just do it before the stage and bring proof.

Awards will be handed out in 4 categories for predesign and one (1) for anything designed during contest hours. There will also be a People's Choice category where the winner is anyone's guess:

Digital (electronic, led, etc)

Smart wear (interactive, temperature sensing, mood changing, etc) Aesthetics (3d printed, geeky wear, passive design)

Miscellaneous (obfuscation, lock picks, shims, card skimmers) Live creations

People's Choice

Judgement based on, but not limited to:

Uniqueness

Trendy

Practical

Couture

Creativity

Relevance

Originality

Presentation

Mastery

Forum: <https://forum.defcon.org/node/232893>

Discord: <https://discord.com/channels/708208267699945503/711644666239647824>

Twitter: <https://twitter.com/Hack3rRunway>

Web: <https://hack3rrunway.github.io>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: H@cker Runw@y

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

For the second year, H@ck3r Runw@y is bringing together fashionistas out there. Make it SMART, LIGHT it up, OBFUSCATE something, or be GEEKY on fleek. Enter clothing, shoes, jewelry, hats or accessories. If you wear it, the runway can handle it. Predesign entry or create something on the fly. Just do it before the stage and bring proof.

Awards will be handed out in 4 categories for predesign and one (1) for anything designed during contest hours. There will also be a People's Choice category where the winner is anyone's guess:

Digital (electronic, led, etc)

Smart wear (interactive, temperature sensing, mood changing, etc) Aesthetics (3d printed, geeky wear, passive design)

Miscellaneous (obfuscation, lock picks, shims, card skimmers) Live creations

People's Choice

Judgement based on, but not limited to:

Uniqueness

Trendy

Practical

Couture

Creativity

Relevance

Originality

Presentation

Mastery

Forum: <https://forum.defcon.org/node/232893>

Discord: <https://discord.com/channels/708208267699945503/711644666239647824>

Twitter: <https://twitter.com/Hack3rRunway>

Web: <https://hack3rrunway.github.io>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: H@cker Runw@y

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

For the second year, H@ck3r Runw@y is bringing together fashionistas out there. Make it SMART, LIGHT it up, OBFUSCATE something, or be GEEKY on fleek. Enter clothing, shoes, jewelry, hats or accessories. If you wear it, the runway can handle it. Predesign entry or create something on the fly. Just do it before the stage and bring proof.

Awards will be handed out in 4 categories for predesign and one (1) for anything designed during contest hours. There will also be a People's Choice category where the winner is anyone's guess:

Digital (electronic, led, etc)

Smart wear (interactive, temperature sensing, mood changing, etc) Aesthetics (3d printed, geeky wear, passive design)

Miscellaneous (obfuscation, lock picks, shims, card skimmers) Live creations

People's Choice

Judgement based on, but not limited to:

Uniqueness

Trendy

Practical

Couture

Creativity

Relevance

Originality

Presentation

Mastery

Forum: <https://forum.defcon.org/node/232893>

Discord: <https://discord.com/channels/708208267699945503/711644666239647824>

Twitter: <https://twitter.com/Hack3rRunway>

Web: <https://hack3rrunway.github.io>

[Return to Index](#) - Add to  - ics [Calendar file](#)

HTS - Saturday - 11:00-11:59 PDT

Title: Hack the SeaPod

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: Hack the Sea Vlg

SpeakerBio: Grant Romundt

No BIO available

Description: No Description available

Hack the Sea Village activities will be streamed to Twitch.

Twitch: <https://twitch.tv/hackthesea>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HTS - Sunday - 11:00-11:59 PDT

Title: Hack the SeaPod

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: Hack the Sea Vlg

SpeakerBio:Fathom5

No BIO available

Description:No Description available

Hack the Sea Village activities will be streamed to Twitch.

Twitch: <https://twitch.tv/hackthesea>

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Saturday - 11:30-11:59 PDT

Title: Hack-a-Fax

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: Voting Vlg

Speakers:Forrest Senti,Mattie Gullixson,Caleb Gardner

SpeakerBio:Forrest Senti , Director of Business & Government Affairs, National Cybersecurity Center

No BIO available

SpeakerBio:Mattie Gullixson , Secure the Vote Project Manager, National Cybersecurity Center

No BIO available

SpeakerBio:Caleb Gardner , NCC Research Fellow, National Cybersecurity Center

No BIO available

Description:

Millions of overseas voters must choose between the following ballot return methods: international mail, email or fax return as allowed by each respective state law. The insecurity of email and fax, arguably, creates a security gap in the overall elections infrastructure that undermines its integrity. The National Cybersecurity Center proposes to ‘hack a fax’ in order to demonstrate the lack of security, and create an opportunity to strengthen standards. The concern to the broader community is that as we continue to seek to make voting more accessible, it must also be secure. Policies that limit overseas voters to technology that may not have security standards in place, and therefore are insecure, reduces the integrity of the overall elections ecosystem.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

Return to Index - Add to  - ics [Calendar](#) file

AEV - Sunday - 14:00-14:59 PDT

Title: Hack-A-Sat Closing Segment

When: Sunday, Aug 9, 14:00 - 14:59 PDT

Where: Aerospace Vlg

Description:

This segment will officially end the Hack-A-Sat competition. Tune in for awards and celebrations!

This event will be coordinated on the DEF CON Discord server, in channel #av-hack-a-sat-text.

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

Return to Index - Add to  - ics [Calendar](#) file

AEV - Saturday - 16:00-16:30 PDT

Title: Hack-A-Sat End Of Day Recap

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: Aerospace Vlg

Description:

This segment will provide a round-up of the day's Hack-A-Sat activities, notable achievements and other information for the rest of the competition.

This event will be coordinated on the DEF CON Discord server, in channel #av-hack-a-sat-text.

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AEV - Friday - 16:00-16:30 PDT

Title: Hack-A-Sat Friday Recap

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: Aerospace Vlg

Description:

Recap of Friday's Hack-A-Sat competition and a look ahead to Saturday.

This event will be coordinated on the DEF CON Discord server, in channel #av-hack-a-sat-text.

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

Return to Index - Add to  - ics [Calendar](#) file

Title: Hack-A-Sat Kickoff Segment

When: Saturday, Aug 8, 09:00 - 09:30 PDT

Where: Aerospace Vlg

Description:

The daily kickoff for Hack-A-Sat informs attendees of the day's schedule and activities for the competition. Tune in if you want to follow the CTF.

This event will be coordinated on the DEF CON Discord server, in channel #av-hack-a-sat-text.

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AEV - Friday - 08:00-08:25 PDT

Title: Hack-A-Sat Launch Party

When: Friday, Aug 7, 08:00 - 08:25 PDT

Where: Aerospace Vlg

Description:

Overview of the Hack-A-Sat competition, teams and CTF challenges.

This event will be coordinated on the DEF CON Discord server, in channel #av-hack-a-sat-text.

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hack-a-Sat

When: Friday, Aug 7, 08:30 - 15:59 PDT

Where: Aerospace Vlg

Description:

The democratization of space has opened up a new frontier for exploration and innovation. But with this opportunity, new cybersecurity vulnerabilities are also being created. One human can design, build and launch a satellite, adhering to very few standards and security protocols. So how can we achieve safe, reliable and trustworthy operations to truly realize the promise of space?

...BY HACKING A SATELLITE

The United States Air Force, in conjunction with the Defense Digital Service, presents this year's Space Security Challenge, Hack-A-Sat. This challenge asks hackers from around the world to focus their skills and creativity on solving cybersecurity challenges on space systems.

Security experts from around the globe are invited to pull together a team for our Hack-A-Sat Capture the Flag contest. Participants who successfully complete a set of qualification challenges on cybersecurity and space this spring will be invited to the ultimate challenge: to (ethically) hack a satellite.

Forum: <https://forum.defcon.org/node/231203>

Twitter: <https://twitter.com/hackasat>

Web: <https://www.HackASat.com>

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hack-a-Sat

When: Saturday, Aug 8, 09:30 - 15:59 PDT

Where: Aerospace Vlg

Description:

The democratization of space has opened up a new frontier for exploration and innovation. But with this opportunity, new cybersecurity vulnerabilities are also being created. One human can design, build and launch a satellite, adhering to very few standards and security protocols. So how can we achieve safe, reliable and trustworthy operations to truly realize the promise of space?

...BY HACKING A SATELLITE

The United States Air Force, in conjunction with the Defense Digital Service, presents this year's Space Security Challenge, Hack-A-Sat. This challenge asks hackers from around the world to focus their skills and creativity on solving cybersecurity challenges on space systems.

Security experts from around the globe are invited to pull together a team for our Hack-A-Sat Capture the Flag contest. Participants who successfully complete a set of qualification challenges on cybersecurity and space this spring will be invited to the ultimate challenge: to (ethically) hack a satellite.

Forum: <https://forum.defcon.org/node/231203>

Twitter: <https://twitter.com/hackasat>

Web: <https://www.HackASat.com>

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hack-a-Sat

When: Sunday, Aug 9, 09:00 - 13:59 PDT

Where: Aerospace Vlg

Description:

The democratization of space has opened up a new frontier for exploration and innovation. But with this opportunity, new cybersecurity vulnerabilities are also being created. One human can design, build and launch a satellite, adhering to very few standards and security protocols. So how can we achieve safe, reliable and trustworthy operations to truly realize the promise of space?

...BY HACKING A SATELLITE

The United States Air Force, in conjunction with the Defense Digital Service, presents this year's Space Security Challenge, Hack-A-Sat. This challenge asks hackers from around the world to focus their skills and creativity on solving cybersecurity challenges on space systems.

Security experts from around the globe are invited to pull together a team for our Hack-A-Sat Capture the Flag contest. Participants who successfully complete a set of qualification challenges on cybersecurity and space this spring will be invited to the ultimate challenge: to (ethically) hack a satellite.

Forum: <https://forum.defcon.org/node/231203>

Twitter: <https://twitter.com/hackasat>

Web: <https://www.HackASat.com>

Discord: <https://discord.com/channels/708208267699945503/732393766677119087>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CNE - Friday - 18:00-19:59 PDT

Title: Hacker Jeopardy

When: Friday, Aug 7, 18:00 - 19:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/232964>

Discord: <https://discord.com/channels/708208267699945503/732439600391389184>

Twitch: <https://www.twitch.tv/dfiutv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CNE - Saturday - 18:00-19:59 PDT

Title: Hacker Jeopardy

When: Saturday, Aug 8, 18:00 - 19:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/232964>

Discord: <https://discord.com/channels/708208267699945503/732439600391389184>

Twitch: <https://www.twitch.tv/dfiutv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: HackerBox 0057 Build Session

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Joseph Long (hwbxr)

Joseph Long (hwbxr) is the founder of HackerBoxes: the monthly subscription box for DIY electronics, computer technology, and hacker culture. He has extensive experience in technology R&D and is an attorney of technology law. A former member of the research faculty at Georgia Tech, Joseph is a licensed professional engineer, amateur radio volunteer examiner, past IEEE senior member and chair of multiple IEEE chapters. He has directed or contributed to numerous engineering projects in diverse technology areas including digital and embedded systems, medical devices, broadband communications, and information security. Joseph has provided engineering expertise to technology startups, Fortune 500 companies, NASA, various other government agencies, and research laboratories. He has also prepared and prosecuted hundreds of patent applications for technology leaders such as Google, Microsoft, IBM, AT&T, Cisco, and Boeing as well as technology startups and various university clients.

Description:

Build HackerBox 0057 to explore microcontroller programming, IoT WiFi exploits, Bluetooth control, IR hacks, lockpicking tools, audio/video signaling, and more. HackerBoxes are the monthly subscription box for DIY electronics and computer technology. Each monthly HackerBox is a surprise. But this month the cathode is out of the bag, so to speak. The theme is SAFE MODE.

There will be an indie badge kit featuring dual core ESP32, IPS full-color 240x135 display, AV out, IR in/out, micro joystick, USB-C interface, battery charger, Wi-Fi, Bluetooth, and it's Arduino programmable. Of course there will be swag galore. HackerBox 0057 will bring home a "village" of IoT, Wireless, Lockpicking, and of course Hardware Hacking that should not disappoint.

Monthly HackerBoxes usually ship around the last day of the month. However, SAFE MODE HackerBox 0057 will ship a few days early (for both existing a new members) and should be received in time for DEF CON 28 SAFE MODE. We recommend ordering by July 22, but earlier is always better in light of recent postal delays.

#hhv-badgebuddy-qa-text: <https://discord.com/channels/708208267699945503/709254868329693214>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: HackerBox 0057 Build Session

When: Sunday, Aug 9, 11:30 - 12:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Joseph Long (hwbxr)

Joseph Long (hwbxr) is the founder of HackerBoxes: the monthly subscription box for DIY electronics, computer technology, and hacker culture. He has extensive experience in technology R&D and is an attorney of technology law. A former member of the research faculty at Georgia Tech, Joseph is a licensed professional engineer, amateur radio volunteer examiner, past IEEE senior member and chair of multiple IEEE chapters. He has directed or contributed to numerous engineering projects in diverse technology areas including digital and embedded systems, medical devices, broadband communications, and information security. Joseph has provided engineering expertise to technology startups, Fortune 500 companies, NASA, various other government agencies, and research laboratories. He has also prepared and prosecuted hundreds of patent applications for technology leaders such as Google, Microsoft, IBM, AT&T, Cisco, and Boeing as well as technology startups and various university clients.

Description:

Build HackerBox 0057 to explore microcontroller programming, IoT WiFi exploits, Bluetooth control, IR hacks, lockpicking tools, audio/video signaling, and more. HackerBoxes are the monthly subscription box for DIY electronics and computer technology. Each monthly HackerBox is a surprise. But this month the cathode is out of the bag, so to speak. The theme is SAFE MODE.

There will be an indie badge kit featuring dual core ESP32, IPS full-color 240x135 display, AV out, IR in/out, micro joystick, USB-C interface, battery charger, Wi-Fi, Bluetooth, and it's Arduino programmable. Of course there will be swag galore. HackerBox 0057 will bring home a "village" of IoT, Wireless, Lockpicking, and of course Hardware Hacking that should not disappoint.

Monthly HackerBoxes usually ship around the last day of the month. However, SAFE MODE HackerBox 0057 will ship a few days early (for both existing a new members) and should be received in time for DEF CON 28 SAFE MODE. We recommend ordering by July 22, but earlier is always better in light of recent postal delays.

#hhv-badgebuddy-qa-text: <https://discord.com/channels/708208267699945503/709254868329693214>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hackers And ISACS

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Aerospace VIg

Speakers:Erin Miller,Jeff Troy,Ken Munro,Matthew Gaffney,Pete Cooper

SpeakerBio:Erin Miller , VP of Operations for Space ISAC, National Cybersecurity Center

Erin has over a decade of experience building meaningful tech collaborations and has formed hundreds of formal partnerships between government, industry and academia to solve problems for warfighters and national security. Currently Erin is building a Public-Private Partnership (P3), called Space ISAC. This is the third non-profit launch Erin has led and has been passionate about P3 for her entire career.

Erin was the Managing Director of the Center for Technology, Research and Commercialization (C-TRAC) and brought three USAF-funded programs to bear at the Catalyst Campus for Technology & Innovation (www.catalystcampus.org) from 2016-2018. Her expertise in brokering unique partnerships using non-FAR type agreements led to the standup of the Air Force's first cyber focused design studio, AFCyberWorx at the United States Air Force Academy, and the first space accelerator, Catalyst Accelerator, at Catalyst Campus in Colorado Springs - in partnership with Air Force Research Laboratory and AFWERX.

In 2018 Erin was recognized by the Mayor of Colorado Springs as Mayor's Young Leader (MYL) of the Year Award for Technology. She is also the recipient of Southern Colorado Women's Chamber of Commerce Award for Young Female Leader in 2018. Erin serves on the board of cyber teaching certifications at Handshake Leadership. A company putting purpose over profit.

SpeakerBio:Jeff Troy , President, CEO, Aviation ISAC

Over the past three years, Jeff developed the A-ISAC comprehensive strategy, led the team's expansion of the Aviation ISACs services, and tripled membership. He established relationships with global regulators, industry associations, and private sector companies to drive cyber risk reduction across the aviation eco-system. Concurrently, Jeff employed by General Electric and is on the Board of Directors, National Defense ISAC. ND-ISAC provides cutting edge cyber security training, intelligence development and a trusted information sharing environment for US cleared defense contractors. Jeff spent 25 years as a Special Agent of the FBI. He retired as the Deputy Assistant Director for Cyber National Security and Cyber Criminal Investigations.

SpeakerBio:Ken Munro

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 Aviation Village, the Global Connected Aircraft Summit, and the Aviation ISAC Summit among others.

SpeakerBio:Matthew Gaffney , Managing Director, BSSI UK

Matt is an aviation cybersecurity consultant at BSSI UK where he also holds the position of Managing Director. He started his cybersecurity career whilst serving in the British Army after being volunteered for a mandatory IT Security Officer course because he 'has some experience with IT'. With more than 14 years experience across multiple industries from Military and Government to banking and aviation, Matt has mostly worked on the entry into service of e-Enabled aircraft at the operator (airline) level. Due to this, his focus is primarily on systems implemented by the operator and whose touchpoints are the Aircraft Information Systems Domain (AISD). His particular areas of interest are the Electronic Flight Bag (EFB) and ground systems. A relative newbie to the research field, he recently released his first paper 'Securing e-Enabled aircraft information systems' and plans on releasing others in the coming months.

SpeakerBio:Pete Cooper

Pete Cooper - Dir Aerospace Village. His first tech love was a ZX Spectrum but then he then moved on to flying fast jets in the UK Royal Air Force. Then he moved into cyber operations before leaving the military 4 years ago. Since then he has started up his own cyber security firm and has advised on everything from developing global cyber security strategies with UN bodies such as ICAO, advising the ICRC on the nature of state vs state cyber conflict and also enjoys playing with active cyber defence and deception. Pete is also the founder and Dir of the UK Cyber Strategy Challenge “Cyber9/12”, holds an MSc in Cyberspace Operations, is a Senior Fellow at Kings College London, a Non-Resident Senior Fellow at the Atlantic Council Cyber Statecraft Initiative and a Fellow of the Royal Aeronautical Society.

Description:

Across the aerospace sector, good faith research has a key role in highlighting both risks and vulnerabilities but it hasn't always been welcomed with open arms. ISACs are often seen as a key point of contact for researchers and hackers doing this work but how best do we create relationships across hackers and ISACs to learn the lessons of the past and build the trust that we need?

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hackfortress

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

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 solving puzzles. 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.

Forum: <https://forum.defcon.org/node/232291>

Discord: <https://discord.com/channels/708208267699945503/711643831275225125>

Twitter: <https://twitter.com/tf2shmoo>

Web: <http://hackfortress.net>

Return to Index - Add to  - ics [Calendar](#) file

Title: Hackfortress

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

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 solving puzzles. 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.

Forum: <https://forum.defcon.org/node/232291>

Discord: <https://discord.com/channels/708208267699945503/711643831275225125>

Twitter: <https://twitter.com/tf2shmoo>

Web: <http://hackfortress.net>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hackfortress

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

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 solving puzzles. 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.

Forum: <https://forum.defcon.org/node/232291>

Discord: <https://discord.com/channels/708208267699945503/711643831275225125>

Twitter: <https://twitter.com/tf2shmoo>

Web: <http://hackfortress.net>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Aerospace Cybersecurity Regulation

When: Sunday, Aug 9, 09:00 - 09:59 PDT

Where: Aerospace VIg

Speakers:Harley Geiger,Kaylin Trychon,Nicky Keeley

SpeakerBio:Harley Geiger , Director of Public Policy, Rapid7

Harley Geiger is Director of Public Policy at Rapid7, where he leads the company's policy engagement on cybersecurity, encryption, computer crime, exports, and digital trade issues. Prior to working at Rapid7, Geiger was Advocacy Director at the Center for Democracy & Technology (CDT), where he worked on issues related to government surveillance, privacy and computer crime. Prior to that, Geiger was Senior Legislative Counsel for U.S. Representative Zoe Lofgren of California, serving as lead staffer for technology policy. Geiger is an attorney and is CIPP/US certified.

SpeakerBio:Kaylin Trychon

No BIO available

SpeakerBio:Nicky Keeley , Head of Cyber Security Oversight, Civil Aviation Authority

Nicole leads the team responsible for regulatory cyber security oversight, for aviation in the UK. Her aim is to have a proportionate and effective approach that enables aviation to manage cyber security risks without compromising aviation safety, security or resilience (with a particular focus on critical national infrastructure). Having worked in a variety of industries in various GRC and technical information security roles, she loves the interconnected and diverse nature of aviation.

Description:

The aerospace industry is highly regulated with a great deal of focus on cybersecurity. Other sectors have seen how good faith hackers and researchers can help increase resilience and highlight vulnerability – how best to do that in a highly regulated, safety critical industry like aerospace? Aerospace regulators have a key role in understanding risk and putting in place the legal frameworks and creating rules, regulations and best practice around good faith research, join us on a panel with the research community and aerospace regulators to chat about what where we are and what we need to do.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Airplane Air To Ground (A2G) Systems

When: Sunday, Aug 9, 08:30 - 08:59 PDT

Where: Aerospace Vlg

SpeakerBio: Ali Abdollahi

Ali Abdollahi is a cyber security expert with over 8 years of experience working in a variety of security fields. Ali is a full-time consultant helping clients with product security testing, reverse engineering, penetration testing, exploit developing, red-teaming, secure coding, and more, giving him ample opportunity to use his skills in a diversity of ways. In addition, He is instructor, author and board of review at Hakin9 company. Ali is a self-confessed bug hunter, publisher of many vulnerabilities and CVEs. Ali is a regular speaker and trainer at industry conferences.

Twitter: [@AliAbdollahi2](#)

Description:

One of the most important parts of avionic systems is the communication. Airplanes use mobile communication to connect to stations on the ground. In many cases the connection is based on LTE-Advanced technology and in some cases when an airplane is on the seas or somewhere else that there is no base station on the ground, It uses the satellite as a hub. In this presentation I will explain vulnerabilities and ways to take advantage of A2G systems and other avionic components.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Democracy II: On Securing an Election Under Times of Uncertainty and Upheaval

When: Friday, Aug 7, 11:30 - 12:30 PDT

Where: Voting VIg

Speakers: Casey John Ellis, Kimber Dowsett, Tod Beardsley, Jack Cable, Amèlie Koran

SpeakerBio: Casey John Ellis , Founder and CTO, Bugcrowd

Casey Ellis is the Founder, Chairman and CTO of Bugcrowd and the co-founder of the The disclose.io Project. Casey has been making computers, companies, and markets misbehave for great justice since his youth, and pioneered the crowdsourced security-as-a-service industry in 2012.

SpeakerBio: Kimber Dowsett , Director of Security Engineering, Truss

No BIO available

SpeakerBio: Tod Beardsley , Director of Research, Rapid7

No BIO available

SpeakerBio: Jack Cable , Election Security Technical Advisor, U.S. CISA

No BIO available

SpeakerBio: Amèlie Koran , Senior Technology Advocate, Splunk

No BIO available

Description:

Democracy is the cornerstone of America's Constitution, identity, and ideology, and this foundation was shaken during the 2016 Presidential Election. Four years later, we still have great lengths to go to ensure that the integrity of the 2020 Presidential Election, and any election moving forward, is protected.

In February, this panel convened to discuss the threats and challenges that are present and may arise between then and the November election. We discussed the intersection of people, technology, security, and elections, with a focus on themes including:

- The true scope of the problem when it comes to “hacking elections
- The biggest threats to the 2020 vote—threat modeling for disinformation, voting machine vulnerabilities, website hacking, and election manipulation
- The role of hackers and coordinated vulnerability disclosure in building voter trust and improve cyber-resilience
- The impact for the elections in the west at large, driven by the U.S.'s prominence as the champion for democracy.

However, we did not know a pandemic and a constantly changing rhetoric by candidates and government leaders, along with several court cases, primaries and other events would add even more challenges for the 2020 election. We will discuss what is left in the 90 days left between now and the election, what can be feasibly helped by the public, governments, and others to ensure a secure and valid election, as well as what will need to be carried forward as lessons learned.

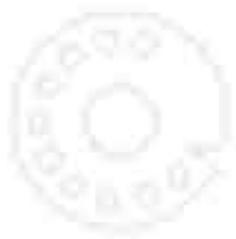
YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

Return to [Index](#) - Add to  - ics [Calendar](#) file

DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON

Title: Hacking like Paris Hilton 14 years later - and still winning!

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio:Per Thorsheim

Per Thorsheim is the founder of PasswordsCon. By day he works as CSO of a large hotel chain in northern europe, holds multiple relevant certifications & bla bla bla. By evening, night, weekends & vacations he is passionate about passwords, digital authentication, email & DNS security/privacy.

He has spoken at conferences in many countries around the world (including Cryptovillage!), and is frequently interviewed in media. He is known for his passionate & easy to understand presentations, mixing technical topics with humor, stories from real life & practical advice.

Description:

Simswap attacks has increased in recent years, with several high-profile cases in the media showing very fast & effective ways of duping people or getting access to valuable accounts . All the way back in 2006 Paris Hilton got accused of hacking into the voicemail of Lindsay Lohan, while similar scandals has been observed since then in other countries as well.

Asking around in my home country of Norway, neither simswap attacks or voicemail hacking seemed to be known among most infosec people, or at least not part of anyone's risk analysis. So I decided to take a closer look.

The results were shocking at many levels, from technical levels to political decisions & apathy. Several million customers of 3 different carriers in 3 countries were exposed to potential voicemail hacking for up to 13 years. A fake business card was enough to do a simswap & hijack the number of a famous female blogger, while credential stuffing against a mobile carrier allowed for account hijacking of women who used SMS 2FA with their accounts at various services.

This talk will explain what I found, what I did, and how it changed carriers, government agencies, politics & law.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Ludicrous Mode on a Tesla (moar power!)

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: Car Hacking VIg 001

SpeakerBio: Patrick Kiley , Principal Security Consultant, Rapid7

Patrick Kiley (GXPN, GPEN, GAWN, GCIH, CISSP, MCSE) has over 18 years of information security experience working with both private sector employers and the Department of Energy/National Nuclear Security Administration (NNSA). While he was with the NNSA he built the NNSA's SOC and spent several years working for emergency teams. Patrick has performed research in Avionics security and Internet connected transportation platforms. Patrick has experience in all aspects of penetration testing, security engineering, hardware hacking, IoT, Autonomous Vehicles and CAN bus.

Twitter: [@gigstorm](https://twitter.com/gigstorm)

Description:

This talk will cover how I reverse engineered the ludicrous upgrade process on the P85D. I then successfully upgraded the hardware and firmware on a P85D to make the car faster. I will cover the hardware upgrades, the firmware changes as well as the architecture of the Tesla Battery Management System.

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUejlQ&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking Security Leadership

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: Career Hacking Vlg

SpeakerBio:Pete Keenan

No BIO available

Description:

So you are a great hacker who can pop shells all day and make the IT team weep. At some point, that will have diminishing returns for both you and the company you serve. Every one of us has delivered or received that dreaded vulnerability report with 100,000+ items on it and heard (or made) that desperate sigh of defeat. Too many times we perform amazing red team work and deliver reports full of detailed findings, only to come back a year later and see nothing has been fixed. Breaking things is the easy part; how do you drive change when you don't have direct authority? Our goal is to make an enterprise or product more secure while not driving it out of business and alienating everyone along the way.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking smart-devices for fun and profit: From exploiting my smart-home into controlling thousands of smart-devices around the world

When: Saturday, Aug 8, 09:00 - 09:45 PDT

Where: IOT VIg

SpeakerBio:Barak Sternberg

Barak Sternberg is an Experienced Security Researcher who specializes in Offensive Security. Previously, he spent five years at Unit 8200, as an officer, PO and team leader of security researchers.

Barak is highly-skilled in cyber-security, from vulnerabilities research in various areas (IoT, embedded devices, Linux and web apps) to analyzing malware in the wild. Barak also acquires MSC (in CS) focused on algorithms from Tel-Aviv University.

Description:

Smart-devices are anywhere, connecting lights, AC, cameras and even heat-sensors. They present a weak spot in which hackers can hack and learn about internal network-configuration, change arbitrary controllers, and lead to high physical & software damage. In our scenario, thousands of HDL smart devices could have been exploited & remotely controlled in the wild. 4 unique vulnerabilities have been found and presented here - We show how they can be utilized by a sophisticated attacker to stealth-access smart-devices remotely, change, control and take advantage of their data. Also, we show how a full data-extraction of smart-devices managing accounts: private data and credentials could have been extracted as well. This unique attack scenario demonstrates the high-security impact of deploying IoT devices over any organization, especially when using dedicated IoT hardware and proprietary components which are interconnected and even remotely managed. A coordinated responsible disclosure was done and thankful to HDL responsiveness & approach - All was fixed.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking TESLA Model 3 - NFC Relay Revisited

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Car Hacking Vlg 001

Speakers: Huajiang "Kevin2600" Chen, Yuchao (Alex) Zhang

SpeakerBio: Huajiang "Kevin2600" Chen

Huajiang "Kevin2600" Chen (Twitter: @kevin2600) is a senior security researcher at the Ingeek security research lab. He mainly focuses on vulnerability research in wireless and embedded systems. Kevin2600 has spoken at various conferences including XCON; KCON; DEFCON; BLACKHAT; CANSECWEST; OZSecCon and BSIDES

Twitter: [@kevin2600](https://twitter.com/kevin2600)

SpeakerBio: Yuchao (Alex) Zhang

Yuchao (Alex) Zhang is a senior security researcher at the Ingeek security research lab. Alex specializes in Vehicle and IOT Pentesting; Android reverse engineering and mobile vulnerability research.)

Description:

NFC technology is widely developed in payment; ticketing and access control systems. In the automobiles key fob field, Tesla Model 3 is one of the modern vehicles using an NFC tag as a digital car key. By implementing such a system, allows owners driving experience much conveniently.

However, on the other hand, attacking methods against the NFC system also emerge endlessly. The NFC Relay attack is one of the top methods. In this talk, we will reveal the research and attack methods for Tesla Model 3 NFC key tag system. By investigating how this feature works, and how to exploit the protocol by a design flaw. By the end of this talk, we will demonstrate the security limitations of such a system. And the attendees will not only understand how to exploit Tesla's NFC key tag system. But can also apply the same research methods for other brands of vehicles with similar NFC technology.

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUej1Q&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking the Hybrid Cloud

When: Thursday, Aug 6, 12:30 - 12:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Sean Metcalf , CTO, Trimarc

Sean Metcalf is founder and CTO at Trimarc (www.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) certification, is a Microsoft MVP, and has presented on Active Directory & Microsoft Cloud attack and defense at security conferences such as Black Hat, BSides, DEF CON, and DerbyCon. He currently provides security consulting services to customers and posts interesting Active Directory security information on his blog, ADSecurity.org.

Twitter: [@Pyrotek3](https://twitter.com/Pyrotek3)

Description:

Most companies have moved into the cloud and on-premises applications and systems remain. This configuration is reasonably referred to as "hybrid"; in the cloud and not at the same time. Hybrid cloud requires integration and communication between the remaining on-prem infrastructure and the new(er) cloud services.

This talk describes several scenarios that appear to subvert typical security and protections which involve federation configuration, Identity Access Management (IAM), and interaction between SaaS and IaaS in the Microsoft Cloud.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BHV - Friday - 15:30-15:59 PDT

Title: Hacking the Insulin Supply Chain To Save Lives

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: BioHacking Vlg

SpeakerBio: Anthony DiFranco

No BIO available

Description: No Description available

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hacking the Supply Chain – The Ripple20 Vulnerabilities Haunt Hundreds of Millions of Critical Devices

When: Thursday, Aug 6, 14:30 - 14:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Ariel Schön, Moshe Kol, Shlomi Oberman

SpeakerBio: Ariel Schön , Security Researcher

Ariel Schön is an experienced security researcher with unique experience in embedded and IoT security as well as vulnerability research.

Ariel is a veteran of the IDF Intelligence Corps, where he served in research and management positions. Currently, he is consuming caffeine and doing security research at JSOF.

SpeakerBio: Moshe Kol , Security Researcher

Moshe Kol Moshe is a wickedly talented security researcher, currently finishing his Computer Science studies at the Hebrew University of Jerusalem. He has many years of networking and security research experience working for the MOD where he honed his skills originally developed at home – as he was led by sheer curiosity into the world of reverse engineering and security research.

SpeakerBio: Shlomi Oberman , CEO, JSOF

Shlomi Oberman is an experienced security researcher and leader with over a decade of experience in security research and product security. In the past few years his interest has been helping secure Software - while it is being written and after it has shipped. Shlomi is a veteran of the IDF Intelligence Corps and has many years of experience in the private sector working with companies who are leaders in their field. He has spoken internationally and his research has been presented in industry conferences such as CodeBlue Tokyo and Hack-In-The-Box as well as other conferences. He is also an experienced teacher, training researchers and engineers in Embedded Exploitation and Secure Coding, as well as an organizer of local community cyber-security events. Shlomi has the unique advantage of a broad technical understanding of the Security Field as well as deep knowledge of the attacker's mindset, which is extremely useful when securing software.

Description:

This is the story of how we found and exploited a series of critical vulnerabilities (later named Ripple20) affecting tens or hundreds of millions of IoT devices across all IoT sector conceivable - industrial controllers, power grids, medical, home, networking, transportation, enterprise, retail, defense, and a myriad of other types of IoT devices, manufactured and deployed by the largest American and international vendors in these fields.

These vulnerabilities were found in a TCP/IP software library located at the very beginning of a complex supply chain and have lurked undetected for at least 10 years, likely much more. Over the past two decades this library has spread around the world by means of direct use as well as indirectly, through "second hand" use, rebranding, collaborations, acquisitions and repackaging, having been embedded and configured in a range of different ways. Many of the vendors indirectly selling and using this library were not aware of their using it. Now that they know, the patch propagation dynamics are very complex and may not be possible in some cases.

This library is a little known, but widely used, embedded library developed by Treck Inc. known for its high reliability, performance, and configurability. Its features make it suitable for real-time operating system usage and low-power devices.

Despite being used by many large, security-aware vendors, these vulnerabilities lay dormant and undiscovered - while actors of all types could have discovered these vulnerabilities by finding one of several bugs in any of the components, exposing hundreds of others immediately. This would provide a field day of affected devices for the picking.

In this presentation, we will discuss one of the vulnerabilities in technical depth, demonstrating an RCE exploit on a

vulnerable device. We will explain how the vulnerabilities became so widespread, and what we still don't know. We will speculate as to why these vulnerabilities survived for so long and show why some vendors are worse affected than others.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Hacking traffic lights

When: Thursday, Aug 6, 13:30 - 13:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Rik van Duijn, Wesley Neelen

SpeakerBio: Rik van Duijn, Hacker & co-founder at Zolder

Rik is a security researcher with 7+ years of experience as a penetration tester. Nowadays Rik focusses on malware research and defense. His hobbies include cooking, bouldering and long walks on the beach. Rik has presented at SHA2017, (whiskeyfristi)leaks, DefCon BlueTeam Village and Tweakers Security/DEV Meetups.

Twitter: [@rikvduijn](https://twitter.com/rikvduijn)

SpeakerBio: Wesley Neelen, Hacker & co-founder at Zolder

Wesley has about 7 years' experience in the offensive security area working as a penetration tester. Next to his work assessing the security of infrastructures, he spends time researching trends within IT security and on developing defensive measures. Wesley likes to actively assess the security of home automation, internet of things and 'smart' innovations. One of the vulnerabilities discovered by Wesley, is a remote command execution (RCE) vulnerability in the Fibaro home center appliance. The vulnerability allowed to remotely obtain root access on the Fibaro device whenever the web interface is reachable. Also, he discovered vulnerabilities within a smartwatch cloud that disclosed the location history of about 300.000 of its users.

Twitter: [@wesleyneelen](https://twitter.com/wesleyneelen)

Description:

New systems are connected to the internet every day to make our lives easier or more comfortable. We are starting to see connected traffic and smart traffic lights innovations to improve traffic flow, safety and comfort. With smart systems entering and controlling our physical world, ethical hacking such systems to find possible ways of manipulation becomes even more important to society.

In the Netherlands there are some public innovations where traffic light systems are being connected to smartphone apps. We have looked at these innovations to see if these systems could be manipulated and how manipulation could benefit an attacker. Specifically, we found a way in two different platforms, that allows us to successfully fake a continuous flow of bicyclists that turns the cyclist traffic light instantly green or decreases the time to green.

More than 10 municipalities in the Netherlands connected a part of their cyclist traffic lights to the affected platforms. It was possible to perform these hacks from any remote location, which allows someone to remotely influence the traffic at scale. The hack results in turning the cyclists lights to green, while other lights on the intersection will turn to red.

The regular security systems that make sure lights are not turned green simultaneously stays intact. There are similar projects that turn the car traffic lights green for ambulances or trucks. If an attacker succeeds to exploit these projects with a similar attack, he could remotely influence the car traffic lights directly.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](https://discord.com/channels/708208267699945503/733079621402099732)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON

AIV - Friday - 14:00-14:50 PDT

Title: Hacking with Skynet - How AI is Empowering Adversaries

When: Friday, Aug 7, 14:00 - 14:50 PDT

Where: AI Vlg

SpeakerBio:GTKlondike

No BIO available

Twitter: [@GTKlondike](https://twitter.com/GTKlondike)

Description:No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Hacking Zoom: a Hacker's Journey into Zoom Security

When: Sunday, Aug 9, 06:00 - 06:59 PDT

Where: Red Team Vlg

SpeakerBio: Mazin Ahmed

Mazin Ahmed is a security consultant who specializes in AppSec and offensive security. He is passionate about information security and has previously found vulnerabilities in Facebook, Twitter, LinkedIn, and Oracle to name a few. Mazin is the developer of a number of popular open-source security tools that have been integrated into security testing frameworks and distributions. Furthermore, Mazin's research of WAF security has earned the 4th place on top web hacking techniques of 2015 award. Mazin also built FullHunt, the next-generation vulnerability intelligence platform.

Description:

Zoom is a popular digital video conferencing company. Zoom has become one of the most valuable companies in the world during the pandemic, with millions of users and hundreds of millions of monthly participants globally. I have done a security research experiment in spare time to test Zoom and to find security risks and vulnerabilities on Zoom. The experiment resulted in interesting findings along with interesting vectors I identified within the journey. In this talk, I will be showcasing my findings and the results of my experiment. I will also discuss some of the challenges in the conducted responsible disclosure.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hackium: a browser for web hackers

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: AppSec Vlg

SpeakerBio:Jarrod Overson

No BIO available

Twitter: [@jsoverson](#)

Description:

The web has changed. Sites went from being a few kilobytes of static, hand-written HTML to monstrosities of tangled JavaScript that eat hundreds of megs of RAM. Web sites are applications now, complete with security controls, complex state, and custom protocols. Our tools need to become smarter.

Hackium is part of a new tool suite designed to both give greater control over browsers and the content they execute, as well as make work more sharable and portable. Hackium itself acts like a CLI-driven browser that runs automation scripts. Add libraries like shift-refactor, a JavaScript transformation library, and shift-interpreter, a JavaScript meta-interpreter, and you can intercept and manipulate JavaScript with just a few lines of code, no proxies necessary. This session will introduce Hackium and how you can use features like the REPL to automate in-page tasks, work with 3rd party APIs for tasks like CAPTCHA solving, and intercept traffic to automatically deobfuscate JavaScript.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

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

Title: Ham Radio USA License Exams (Friday)

When: Friday, Aug 7, 11:00 - 13:59 PDT

Where: See Description or Village

Description:

The Ham Radio Village team is happy to announce that we will be offering virtual license exams this year during DEF CON Safe Mode. The team has negotiated a special discount rate of \$5 for the exams. Additionally, the fee is waived for any applicants that are under the age of 18, a student with a current student ID, active military, or a veteran of the armed forces. Registration for exams is required.

Twitter: https://twitter.com/DC_Ham_Exams

Discord: <https://discord.com/channels/708208267699945503/732733631667372103>

Info/Reg: <https://ham.study/sessions/5f0e7677295c50941c2cad5f/1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Saturday - 14:00-16:59 PDT

Title: Ham Radio USA License Exams (Saturday)

When: Saturday, Aug 8, 14:00 - 16:59 PDT

Where: See Description or Village

Description:

The Ham Radio Village team is happy to announce that we will be offering virtual license exams this year during DEF CON Safe Mode. The team has negotiated a special discount rate of \$5 for the exams. Additionally, the fee is waived for any applicants that are under the age of 18, a student with a current student ID, active military, or a veteran of the armed forces. Registration for exams is required.

Twitter: https://twitter.com/DC_Ham_Exams

Discord: <https://discord.com/channels/708208267699945503/732733631667372103>

Info/Reg: <https://ham.study/sessions/5f0e7799017958f2523dbb97/1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ham Radio USA License Exams (Sunday)

When: Sunday, Aug 9, 15:00 - 17:59 PDT

Where: See Description or Village

Description:

The Ham Radio Village team is happy to announce that we will be offering virtual license exams this year during DEF CON Safe Mode. The team has negotiated a special discount rate of \$5 for the exams. Additionally, the fee is waived for any applicants that are under the age of 18, a student with a current student ID, active military, or a veteran of the armed forces. Registration for exams is required.

Twitter: https://twitter.com/DC_Ham_Exams

Discord: <https://discord.com/channels/708208267699945503/732733631667372103>

Info/Reg: <https://ham.study/sessions/5f0e77d9a47e313e8e5295d9/1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hardware hacking 101: There is plenty of room at the bottom

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Federico Lucifredi

Federico Lucifredi is the Product Management Director for Ceph Storage at 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.

Description:

This is a live demonstration of hacking into the processor embedded in an SD card, effectively turning the device into a potentially covert Raspberry Pi-class computer under your complete control. The ARM926EJ-S ARM processor made its appearance as the embedded CPU in Transcend's WiFi-enabled SD cards, clocking in at an impressive 426 BogoMips – we can't possibly leave that territory unexplored, can we?

In this session we root the card's own CPU, install a more featureful OS, and explore the system's common and unusual capabilities (in hardware AES encryption and native support for Java bytecode among them). These provide plenty of building blocks for our projects.

Clearly, complete control of such a hidden computer running with full network connectivity can be used in network penetration scenarios. We'll discuss applicable security threat countermeasures.

There is plenty of room at the bottom, and opening these computer-within-the computer configurations create interesting miniaturized automation scenarios alongside the obvious, more ominous security aspects.

Use your newfound knowledge for good, with great power comes great responsibility!

#hhv-hw101-talk-qa-text: <https://discord.com/channels/708208267699945503/709255105479704636>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hardware hacking 101: There is plenty of room at the bottom

When: Saturday, Aug 8, 09:30 - 09:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Federico Lucifredi

Federico Lucifredi is the Product Management Director for Ceph Storage at 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.

Description:

This is a live demonstration of hacking into the processor embedded in an SD card, effectively turning the device into a potentially covert Raspberry Pi-class computer under your complete control. The ARM926EJ-S ARM processor made its appearance as the embedded CPU in Transcend's WiFi-enabled SD cards, clocking in at an impressive 426 BogoMips – we can't possibly leave that territory unexplored, can we?

In this session we root the card's own CPU, install a more featureful OS, and explore the system's common and unusual capabilities (in hardware AES encryption and native support for Java bytecode among them). These provide plenty of building blocks for our projects.

Clearly, complete control of such a hidden computer running with full network connectivity can be used in network penetration scenarios. We'll discuss applicable security threat countermeasures.

There is plenty of room at the bottom, and opening these computer-within-the computer configurations create interesting miniaturized automation scenarios alongside the obvious, more ominous security aspects.

Use your newfound knowledge for good, with great power comes great responsibility!

#hhv-hw101-talk-qa-text: <https://discord.com/channels/708208267699945503/709255105479704636>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Hashes; Smothered, Covered, and Scattered: Modern Password Cracking as a Methodology

When: Sunday, Aug 9, 12:15 - 13:15 PDT

Where: Red Team VIg

SpeakerBio: Lee Wangenheim

Lee Wangenheim works as a security consultant for the Attack and Penetration team at Optiv. As part of his job he helps to maintain the teams password crackers as well as perform enterprise password audits for various clients. After fielding several questions from the team about best practices, he set out to define the methodology a modern consultant can use to attack passwords they find on an engagement.

Description:

With the explosion of GPU enabled processing power password cracking has long grown beyond the standard wordlist. New tools and techniques are being used in order to effectively and efficiently crack passwords that just a few years ago would have be unfathomable. People often ask me, what is the best way to crack this hash, and the truth is it really depends. Let us introduce some of the more modern and best ways to attack passwords by analyzing the language structures and character patterns of passwords, as well as developing custom rules and rule chains to maximize effort. Password cracking is one of those things that has been around for a long time, however people often do not associate a methodology behind it and consider it just a tool. My presentation has a large amount of content to cover within a 50-minute window, therefore our demos are light and quick showing the different tools built for cracking locally, in the cloud, or in a distributed environment. I feel that by passing along the knowledge of the ins and outs of the tools will be more valuable than having people watch us crack passwords on the screen. The slide decks can be made available to participants and contains sample commands for them to try out each technique I present.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Have my keys been pwned? - API Edition

When: Sunday, Aug 9, 15:00 - 15:59 PDT

Where: Red Team VIg

Speakers: José Hernandez, Rod Soto

SpeakerBio: José Hernandez

José Hernandez is a Principal Security Researcher at Splunk. He started his professional career at Prolexic Technologies (now Akamai), fighting DDOS attacks from “anonymous” and “lulzsec” against Fortune 100 companies. As an engineering co-founder of Zenedge Inc. (acquired by Oracle Inc.), José helped build technologies to fight bots and web-application attacks. While working at Splunk as a Security Architect, he built and released an auto-mitigation framework that has been used to automatically fight attacks in large organizations. He has also built security operation centers and run a public threat-intelligence service. Although security information has been the focus of his career, José has found that his true passion is in solving problems and creating solutions. As an example, he built an underwater remote-control vehicle called the SensorSub, which was used to test and measure toxicity in Miami's waterways.

SpeakerBio: Rod Soto

Rod Soto worked at Prolexic, Akamai, Caspida. Won BlackHat CTF in 2012. Co-founded Hackmiami, Pacific Hackers meetup and conferences.

Description:

Current status quo of credential management in cloud related DEVOPS environments enables attackers to easily obtain leaked credentials. This presentation showcases how leaked credentials in public repositories can potentially lead to further compromise in enterprise environments. The focus will be on the DEVOPS attack surface and the toolchains involved within this process in cloud platform environments. Presenters will use a recently released tool (Git Wild Hunt) to show how public leaks can lead to further compromise of individuals and enterprises with actual examples of derived information from compromised secrets. An analysis of credentials leaked globally and its source (company affected and user) will be provided as examples.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Heightened Election Security Risks Admist the Pandemic

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: Voting Vlg

Speakers:Jack Cable,Alex Zaheer

SpeakerBio:Jack Cable , Election Security Technical Advisor, U.S. CISA

No BIO available

SpeakerBio:Alex Zaheer , Election Security Technical Advisor, U.S. CISA

No BIO available

Description:

Amidst the COVID-19 pandemic, countless aspects of American life have been impacted, including our elections. Accommodations for the pandemic include an unprecedented shift towards absentee balloting across the United States, as well as drastically reduced in-person voting options. While we cannot predict the state of the pandemic come November, it is clear that elections will operate differently, constrained by health concerns around in-person voting, reduced polling place staff, and massive budget shortfalls. Such large-scale change will necessarily impact election security, as new attack surfaces open due to states relying on rapidly expanded infrastructure. With political polarization at a high, it is crucial that elections remain safe and secure despite the pandemic, and that American citizens believe their elections credible. In this talk, we will explore the areas of election infrastructure that are changing, and new associated security concerns based on our work at the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

Return to [Index](#) - Add to  - ics [Calendar](#) file

IOT - Friday - 14:15-14:59 PDT

Title: Hella Booters: Why IoT Botnets Aren't Going Anywhere

When: Friday, Aug 7, 14:15 - 14:59 PDT

Where: IOT VIg

SpeakerBio: Netspooky

netspooky is a reverse engineer in the ICS and IoT space.

Description:

This talk discusses the rise of IoT botnets, the culture that surrounds them, and the vulnerabilities that enable their continued existence. I will discuss various analyses of major botnet families, discuss exploits and vulnerability classes in IoT devices, and examine the rapid growth of these botnets for commercial use. I will also discuss newer innovations in IoT malware, and outline some of the ways that vendors could reduce their impact moving forward.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: High Security Wafer Locks - An Oxymoron?

When: Saturday, Aug 8, 10:45 - 11:45 PDT

Where: Lockpick Vlg

SpeakerBio:zeefeene

No BIO available

Description:

There's a lot that's been said about the poor quality of common wafer locks which lurk in offices today, but what if I told you there's a wafer lock that's been made since the 1800s, and you don't have a chance of picking it...?

Take a deep dive with me into the wonders and horrors of one of the most secure mechanical locks in the world, and let me show you why wafer locks might just hold the secret to better physical security!

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: HomebrewHardware Contest

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Have you learned how to build your own hacking hardware at home? Are you etching circuit-boards in your lab, or soldering in a toaster oven in your garage? Are you hosting a MUD on your helmet, or making malicious USB hardware? Did you make something to help you in your everyday life, a unique wearable, or something really nefarious? Are you discovering what old boards do, bending circuits, or re-appropriating the innards of your local e-waste?

We want to see the awesome things you've been building over the last year.

The HomebrewHardware competition is a place to showcase your skill, techniques, and project.

Check our website and twitter for this year's rules.

Forum: <https://forum.defcon.org/node/233025>

Discord: <https://discord.com/channels/708208267699945503/711644075110957096>

Twitter: <https://twitter.com/homebrewhardwa1>

Web: <https://homebrewhardwarecontest.github.io/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: HomebrewHardware Contest

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Have you learned how to build your own hacking hardware at home? Are you etching circuit-boards in your lab, or soldering in a toaster oven in your garage? Are you hosting a MUD on your helmet, or making malicious USB hardware? Did you make something to help you in your everyday life, a unique wearable, or something really nefarious? Are you discovering what old boards do, bending circuits, or re-appropriating the innards of your local e-waste?

We want to see the awesome things you've been building over the last year.

The HomebrewHardware competition is a place to showcase your skill, techniques, and project.

Check our website and twitter for this year's rules.

Forum: <https://forum.defcon.org/node/233025>

Discord: <https://discord.com/channels/708208267699945503/711644075110957096>

Twitter: <https://twitter.com/homebrewhardwa1>

Web: <https://homebrewhardwarecontest.github.io/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: HomebrewHardware Contest

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Have you learned how to build your own hacking hardware at home? Are you etching circuit-boards in your lab, or soldering in a toaster oven in your garage? Are you hosting a MUD on your helmet, or making malicious USB hardware? Did you make something to help you in your everyday life, a unique wearable, or something really nefarious? Are you discovering what old boards do, bending circuits, or re-appropriating the innards of your local e-waste?

We want to see the awesome things you've been building over the last year.

The HomebrewHardware competition is a place to showcase your skill, techniques, and project.

Check our website and twitter for this year's rules.

Forum: <https://forum.defcon.org/node/233025>

Discord: <https://discord.com/channels/708208267699945503/711644075110957096>

Twitter: <https://twitter.com/homebrewhardwa1>

Web: <https://homebrewhardwarecontest.github.io/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Houston, we CAV a problem

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Car Hacking VIg 002

SpeakerBio: Vic Harkness

Vic is a security consultant working at F-Secure Consulting in England. She works with a wide variety of tech, but her pet areas are novel networks, facial recognition systems, and novel biometric modalities. Outside of work she enjoys annoying birds, travel (or did), and photography. Find her on Twitter @vicharkness, where she mainly shitposts.

Description:

In the future, connected and autonomous vehicles (CAVs) will be everywhere. A lot of different technologies have been proposed for use in CAV intelligent roadways. This talk presents the results of a literature review which aimed to examine the security of the proposals and standards. The proposed CAM/DENM protocols for maintaining awareness between vehicles are paid particular attention, as well as the use of 802.11p/OCB to create base-stationless ad-hoc networks. The results of threat modelling exercises to examine how an attacker may pivot through CAV networks to reach their goals are also described.

#chv-track002-text: <https://discord.com/channels/708208267699945503/739564953014632579>

YouTube: <https://www.youtube.com/watch?v=5DYhXbWkWoA&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack002>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How Blue Penetrates You

When: Saturday, Aug 8, 11:45 - 12:30 PDT

Where: Cloud Vlg

Speakers: Dani Goland, Mohsan Farid

SpeakerBio: Dani Goland

Dani Goland, at the age of 20 he founded his own boutique company for innovative software and hardware solutions. He is a certified AWS Cloud Solutions Architect. While gaining experience in business and finance, Dani did not neglect his hands-on capabilities in both making and breaking systems. Dani recently relocated from Israel to the United States to study Data Science at the prestigious UC Berkeley. During his studies, Dani founded VirusBay, a collaborative malware research community that skyrocketed amongst the global security community with over 2500 researchers. Dani spoke at numerous cybersecurity conferences such as BlackHat USA, CodeBlue Japan, CONFidence, SEC-T, and more. After serving in the Israeli Defense Forces as a commander of a Field Intelligence unit, Dani went on an 8-month journey across South America. He loves snowboarding, music concerts, and having crazy, breathtaking experiences such as spending 5 days in the Bolivian Jungle with no food or water.

Twitter: [@DaniGoland](https://twitter.com/DaniGoland)

SpeakerBio: Mohsan Farid

Mohsan has over 13 years of experience in the cyber security game. Mohsan has ran the gamut in the security space: from penetration testing as a Rapid7 consultant, pen testing for numerous federal agencies, hacking mobile applications, pentesting Fortune 500 companies, and speaking at cybersecurity conferences such as Defcon, Sec-T, Black Alps, and others. Mohsan's traveled to over 100 countries and counting. When he isn't breaking into things, he likes to travel the globe in search of incredible surf, scuba diving, rock climbing, hiking, and is an avid yogi.

Description:

When we started taking a proactive approach to blue teaming, the number of daily scans by automated vulnerability scanners dropped immensely.

In this talk, we will present the mindset we found useful and the techniques we used to make scanning our applications and infrastructure a slow and manual process.

Starting with blocking path and subdomain enumeration with a couple of lines on the proxy bombarding the banners with randomized content that is not differentiable from real content.

Next, we will simulate known vulnerabilities in a subtle way, allowing attackers to connect, pivot, perform lateral movement, and let them exfiltrate terabytes of useless data, wasting their time, resources, and letting your systems fingerprint their TTPs and IOCs

We had a blast presenting at the cloud village last year, and we have many interesting things cooking for this year!

YouTube: https://www.youtube.com/watch?v=gwBG_oKDINQ

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How COVID19 Changed Our Understanding of Cyber Disaster Medicine

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: BioHacking Vlg

Speakers: Christian “quaddi Dameff, Jeff “r3plicant Tully

SpeakerBio: Christian “quaddi Dameff , MD, Physician & Medical Director of Security at The University of California San Diego

Christian (quaddi) Dameff MD is an Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate) at the University of California San Diego. He is also a hacker, former open capture the flag champion, and prior DEF CON/RSA/Blackhat/HIMSS speaker. Published works include topics such as therapeutic hypothermia after cardiac arrest, novel drug targets for myocardial infarction patients, and other Emergency Medicine related works with an emphasis on CPR optimization. Published security research topics including hacking critical healthcare infrastructure, medical devices and the effects of malware on patient care. This is his sixteenth DEF CON.

Twitter: [@CDameffMD](#)

SpeakerBio: Jeff “r3plicant Tully , MD, Anesthesiologist at The University of California Davis

Jeff (r3plicant) Tully is an anesthesiologist, pediatrician and security researcher with an interest in understanding the ever-growing intersections between healthcare and technology.

Twitter: [@JeffTullyMD](#)

Description:

Evangelists for improved security in healthcare have long been concerned about vulnerabilities and impacts stretching beyond privacy and personal health information into the disruption of care and worsening of patient outcomes. As the healthcare system struggles under the burden of the COVID-19 crisis, are there parallels between pandemic preparedness and response and the aims and objectives of healthcare security? Join quaddi and r3plicant, hackers who have been moonlighting as practicing physicians caring for COVID patients, as they discuss what recent experiences and events have taught them about how to reframe and re-address security challenges with the hard-earned hindsight and wisdom of medicine's collective struggles.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 15:00-15:59 PDT

Title: How I defeated the Western Electric 30c

When: Sunday, Aug 9, 15:00 - 15:59 PDT

Where: Lockpick Vlg

SpeakerBio:N thing

No BIO available

Description:

I will take you through my thoughts, motivation and techniques on how I defeated the infamous Western Electric 30c.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How Independent Security Researchers work with Medical Device Manufacturers - The Bad, The Ugly & The Great (BUG)

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: BioHacking VIg

Speakers: Kyle Erickson, Natali, Peter, Veronica

SpeakerBio: Kyle Erickson

Kyle Erickson, the Director of Product Security & Privacy Engineering, Cardiac Rhythm Heart Failure (CRHF), Medtronic. Leading a team of 10 engineers focused on Pre-Market & Post Market Medical Device Cyber Security. He has over a 10 years of incident response leadership at one of the largest HDOs.

SpeakerBio: Natali

Natali brings over 10 years of experience, both as a researcher and a team leader, in the field of offensive cyber security and software development. After graduating magna cum laude B.Sc. in Computer Science at the age of 19, as part of a special program for gifted and talented kids, Natali was handpicked to an elite technology unit at 8200. As part of her military service, she researched various devices and platforms and designed and implemented mission-critical, zero fault software components. Following her military service, Natali joined Cellebrite, a global company that provides digital intelligence solutions for investigations and operations, as Vulnerability & Security Researcher. Her focus was on reverse engineering of mobile platforms, vulnerability research and exploitation and later on she served as a team leader, focusing on Linux kernel exploitation. Prior to founding Sternum, Natali held several security research related roles, including leading different R&D teams at two global cyber intelligence market leaders. In her (limited) spare time, Natali is a content junkie and writes short fiction stories. Natali holds an M.Sc. in Computer Science from Bar Ilan University.

SpeakerBio: Peter

Peter came from Clever Security, a boutique security research company he founded. Clever Security focused on hardware and software reverse engineering, software defined radio, applied cryptography, exploitation and vulnerability research. Previously, he was CTO at Boldend, a cybersecurity-focused software defense contractor focused on cutting-edge research and development for the US DoD and Intelligence community. Before that, he was VP of Research and Development at Accuvant/Optiv where he led the Applied and Vulnerability Research teams focused on product security auditing, and capability development for the US DoD and Intelligence community. Before that, he was a security researcher with Matasano Security, where he was responsible for the Midwest practice region out of Chicago, IL. Peter's career has focused on attacking the intersection of software and hardware to identify security vulnerabilities in products that most security researchers do not have the skillset to audit. While the vast majority of his work is protected via NDA some bespoke output is listed below.

SpeakerBio: Veronica

Veronica started her forensic career in 2008. She is the Director of Incident Response within DFIRLABS. Veronica is also an Assistant Professor at Noroff University, where she will be given her own Minions to plan her world domination. Veronica holds a Master in Science at Rhodes University in Information Security with specialisation in the forensic analysis of malware. She prides herself in keeping patients safe as this is something which is near to her heart. She is also a cyborg sporting an embedded medical device herself. She also is a DEF CON Goon and she is the founder of DC2751. Her particular research interests include research into security vulnerabilities in medical devices forming part of the Internet of Things, and how these could be exploited by malicious attackers, as well as what types of forensic artefacts could be identified from any attacks. She is extremely passionate about protecting people whose lives depend on these medical devices, and her passion saw her becoming a researcher within an MDM. At her core Veronica is a forensicator and hacker and in love with every bit, byte and nibble of knowledge she has obtained.

Description:

"Hear some of the top Security Researchers share their trials and tribulations with Medical Device Manufacturers.

Topics will include:

How they have succeeded in their interactions with larger organizations and what they are working on next. The success stories and failures of working with Medical Device Manufacturers. How working with diverse backgrounds and being open to researchers has helped one company mature its cybersecurity program. What is a proactive security approach and how can it help anticipate failure? How can we tackle the legacy device problem? Explore new ways the community can bring innovative solutions to Medical Device Security."

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: How to get rights for hackers

When: Friday, Aug 7, 09:15 - 09:45 PDT

Where: IOT VIg

SpeakerBio:Chloé Messdaghi

Chloé Messdaghi is the VP of Strategy at Point3 Security. She is a security researcher advocate who strongly believes that information security is a humanitarian issue. Besides her passion to keep people safe and empowered online & offline, she is driven to fight for hacker rights. She is the founder of WomenHackerz & the President and cofounder of Women of Security (WoSEC), podcaster for ITSP Magazine's The Uncommon Journey, and runs the Hacker Book Club.

Description:

Sixty percent of hackers don't submit vulnerabilities due to the fear of out-of-date legislation, press coverage, and companies misdirected policies. This fear is based on socially constructed beliefs. This talk dives into the brain's response to fear while focusing on increasing public awareness in order to bring legislation that supports ethical hackers, ending black hoodie and ski mask imagery, and encourage organizations to support bilateral trust within their policies.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to Grow a Brain in a Jar - Neuroengineering 101

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: BioHacking Vlg

SpeakerBio:Jack

Jack is a biomedical engineer, implantable hardware developer, and EMT. His research involves developing new tools for studying and interacting with the nervous system, including culture systems for emulating brain regions in miniature outside of the body for bioelectrical and neurochemical study.

Description:

As the organ of consciousness, the brain represents the ultimate target for researchers and biohackers interested in investigating and eventually modifying the human organism. Advanced monitoring systems and - more recently - early prostheses targeting the central nervous system have been developed. At the same time, dramatic progress in cell culture techniques and stem cell differentiation have allowed for the creation of autonomous neural structures and “mini-brains ex-vivo, which have been used for therapeutic purposes, microphysiological studies, and more. Additionally, researchers have worked towards creating electronics that mimic the function of the nervous system to enhance computing capabilities. All three of these thrusts fall under the broader umbrella of neuroengineering. This talk aims to provide a crash course in recent developments in the field of neuroengineering, and to show how some of this research might be replicated in the home lab. Come learn about the bleeding edge of neuroengineering, as these technologies begin to move out of the lab and into the biohacking world, and as the line between human and machine grows ever blurrier.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

Return to Index - Add to  - ics [Calendar](#) file

Title: How to hack SWIFT, SPID, and SPEI with basic hacking techniques (from a Red Team Perspective)

When: Friday, Aug 7, 11:45 - 12:45 PDT

Where: Red Team VIg

SpeakerBio:Guillermo Buendia

Guillermo Buendia is a Red Team Lead in one of the biggest insurance companies in the USA, he has worked for many Financial Institutions for the last 8 years. He has presented his previous research in DEF CON, BSidesLV, BSides Manchester, Hackfest, etc.

Description:

Back in 2018, Financial entities in Mexico were hit by one of the biggest cybersecurity breaches in the history of Mexico, and in 2019 "The Bandidos Hacker Team", who allegedly committed the crime, were captured. But do you really need to be a 1337 H4x0r to compromise those systems? In this talk, I will be sharing (from a Red Team Perspective) How I was compromising the SWIFT, SPID, and SPEI systems in a Financial Institution until I gained root access to all the systems using basic hacking techniques like the pretty good old 1337 days. For the blue teamers, I will be sharing ways to detect these techniques that, although may appear simple, they pose a very challenging scenario to create a detection.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to Start a Movement: Hackers Edition

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: Ethics VIg

SpeakerBio:Chloé Messdaghi

Chloé Messdaghi is the VP of Strategy at Point3 Security. She is a security researcher advocate who strongly believes that information security is a humanitarian issue. Besides her passion to keep people safe and empowered online & offline, she is driven to fight for hacker rights. She is the founder of WomenHackerz & the President and cofounder of Women of Security (WoSEC), podcaster for ITSP Magazine's The Uncommon Journey, and runs the Hacker Book Club.

Description:

This will be a live talk.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How to store sensitive information in 2020?

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Mansi Sheth

Mansi Sheth is a Principal Security Researcher at Veracode Inc. In her career, she has been involved with breaking, defending and building secure applications. Mansi researches various languages and technologies, finds insecure usage in customer code and suggests automation measures in finding vulnerabilities for Veracode's Binary Static Analysis service. She is an avid traveller with the motto "If not now, then when?"

Description:

It goes without saying never ever store personal/sensitive information in clear text. It is also a well-known fact salting, hashing or stretching your information can just provide little offline information cracking protection against contemporary computer architectures and modern brute force attack constructs. Those abreast with this subject would have come across countless advocacy material suggesting to use key derivation functions (KDFs) to store sensitive information.

There are handful of solid KDFs, which are good candidates to use for storing sensitive information such as pbkdf2, bcrypt, scrypt, Argon2. In this talk, lets dive deeper to study some of its underlying crypto, what and how to tune these algorithms with secure input parameter configurations and how to decide which algorithm would be the right choice for your needs? Lastly, I will present some statistics on how well do all these different algorithms compare against each other.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: How we recovered \$XXX,000 in Bitcoin from an encrypted zip file

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Michael Stay, CTO, Pyroflex Corp.

Mike Stay was a reverse engineer and cryptanalyst in the 1990s, worked for six years on Google's security team, and is currently the CTO of Pyroflex Corp.

Twitter: [@metaweta](#)

Description:

About six months ago, a Russian guy contacted me on LinkedIn with an intriguing offer. He had hundreds of thousands of dollars in Bitcoin keys locked in a zip file, and he couldn't remember the password. Could I break into it for him? He found my name by reading an old cryptanalysis paper I wrote nearly 20 years ago. In that attack, I needed five files to break into a zip archive. This one only had two files in it. Was it possible? How much would it cost? We had to modify my old attack with some new cryptanalytic techniques and rent a GPU farm, but we pulled it off. Come hear how.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

Return to Index - Add to  - ics [Calendar](#) file

Title: Hunting for Blue Mockingbird Coinminers

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: Recon Vlg

SpeakerBio:Ladislav B

No BIO available

Description:

During March-May 2020 the Blue Mockingbird group infected thousands of computer systems, mainly in the enterprise environments. There are known incidents in which they exploited the CVE-2019-18935 vulnerability in Telerik Web UI for ASP.NET, then they used various backdoors and finally, they deployed XMRig-based CoinMiners for mining Monero cryptocurrency. Interesting about these cases is the persistence which they used for CoinMiners - lot of techniques including scheduled tasks, services, but also WMI Event Subscription and COR Profilers.

During forensic analysis and incident response process it was possible to find these persistences and many coinminers artifacts, but malware samples responsible for their installation and persistence creation have been missing. However, when we enriched results of the standard malware analysis with the Threat Intelligence data and OSInt, we were able to find the missed pieces of puzzle and reconstruct the original attack chain including the initial exploitation, local privilege exploit, two backdoors, main payload and multiple persistence techniques. Moreover, this research reveal many about the tools, techniques and procedures (TTP) of Blue Mockingbird Threat Actor.

Finally, with more knowledge about the attackers it is possible to collect more samples of coinminers used by them. After next step of reconnaissance we can get insight into profit of their attacks and compare them with the damages caused by these attacks.

Recon Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/c/ReconVillage>

#rv-talks-text: <https://discord.com/channels/708208267699945503/737048009732522014>

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 13:00-13:30 PDT

Title: Hybrid PhySec tools - best of both worlds or just weird?

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: Lockpick Vlg

SpeakerBio:d1dymu5

No BIO available

Description:

A few years ago, I invented lock pick collar stays (#GentleMansLockPicks). Since then, I've had some other ideas of practical, small-form factored lockpicking and bypass tools that I can easily carry. I came up with a few ideas. I'll talk about inspiration, designing, manufacturing, and possible collab projects.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 13:00-13:30 PDT

Title: Hyperlocal Drift detection with Goko: Finding abusers of your Dataset

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: AI Vlg

SpeakerBio:comathematician

No BIO available

Twitter: [@comathematician](https://twitter.com/comathematician)

Description:No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: IAM Concerned: OAuth Token Hijacking in Google Cloud (GCP)

When: Friday, Aug 7, 11:20 - 12:05 PDT

Where: Cloud Vlg

SpeakerBio: Jenko Hwong

Jenko Hwong is on the Threat Research Team at Netskope, focusing on cloud threats/vectors. 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.

Twitter: [@jenkohwong](#)

Description:

Imagine you've protected your production Google Cloud environment from compromised credentials, using MFA and a hardware security key. However, you find that your GCP environment has been breached through hijacking of OAuth session tokens cached by gcloud access. Tokens were exfiltrated and used to invoke API calls from another host. The tokens were refreshed by the attacker and did not require MFA. Detecting the breach via Stackdriver was confusing, slowing incident response. And revoking the active OAuth sessions required finding OAuth tokens from logs and using a REST API call, causing further delays in remediation.

This talk will demonstrate a compromised credential attack in Google Cloud Platform by:

- hijacking cached OAuth tokens stored on a GCP administrator's client machine and
- reusing existing gcloud CLI sessions to gain access to multiple GCP environments
- showing that MFA does not apply to OAuth token refreshes for cached credentials (only the initial login)

The POC takes advantage of several issues with GCP IAM design or configuration: OAuth tokens are cached and unencrypted, allowing easy access once the client endpoint has been exploited.

- Tokens can have long or no expiration, allowing potentially long time windows for compromise.
- The attacker can easily refresh tokens, allowing persistence.
- Token refresh does not require MFA making it easy to maintain persistence, creating a false sense of security when MFA is enabled.
- Authentication and Access policies are defined in different admin areas, are confusing, and easily misconfigured.
- Configuring Stackdriver Logging is confusing, leading to slow or ineffective incident response.
- OAuth tokens cannot be revoked easily making remediation difficult.

We will discuss various approaches and challenges to defending:

1. Prevention

- ◆ MFA is not required to refresh the OAuth token
- ◆ Google cloud session timeout (GSuite Admin)
- ◆ IP whitelisting (using VPC Service Controls and Access Context Manager)
- ◆ Explicit client-side revokes (manual)

2. Detection

- ◆ Stackdriver logging data access events must be enabled for all services or else the abuse of OAuth tokens will not be logged and remediation will not be possible.
- ◆ Periodic audit checks on the logs or IAM configurations can be somewhat useful for compliance, but are not real-time so are of limited use for detection.

3. Remediation

- ◆ OAuth tokens can be revoked, but there are caveats: + `gcloud auth revoke` only works on the compromised user's endpoint and requires the user account in order to look up the locally cached OAuth token. This will fail if the attacker deletes the gcloud credential cache. + A REST API revoke call works and

requires the OAuth token, so reliable logging and event parsing must be implemented to ensure tokens can be extracted quickly for IR.

- ◆ Deletion of user accounts has a huge impact.
- ◆ Browser sessions can be revoked but does not apply to Google Cloud sessions.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ictre Normal

When: Friday, Aug 7, 20:00 - 20:59 PDT

Where: See Description or Village

Description:

Ictre has been a premier jubilation hacker, and party host since DEF CON X. People are still talking about the various shenanigans he's orchestrated and videos he's played. Even with this long history, it's still amazing how many people have to still tell him to turn it down. For what?

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Facebook: <https://www.facebook.com/icetre.normal/>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: ICS Hack the Plan[e]t

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Hack the Plan[e]t Capture the Flag (CTF) contest will feature Howdy Neighbor and the Industrial Control System (ICS) Range. This first of its kind CTF will integrate both Internet of Things (IoT) and ICS environments with interactive components for competitors to test their skills and knowledge.

Howdy Neighbor is an interactive IoT CTF challenge where competitors can test their hacking skills and learn about common oversights made in development, configuration, and setup of IoT devices. Howdy Neighbor is a miniature home - made to be “smart” from basement to garage. It’s a test-bed for reverse engineering and hacking distinct consumer-focused smart devices, and to understand how the (in)security of individual devices can implicate the safety of your home or office, and ultimately your family or business. Within Howdy Neighbor there are over 25 emulated or real devices and over 50 vulnerabilities that have been staged as challenges. Each of the challenges are of varying levels to test a competitors ability to find vulnerabilities in an IoT environment. Howdy Neighbor’s challenges are composed of a real or simulated devices controlled by an App or Network interface and additional hardware sensors; each Howdy Neighbor device contains 1 to 3 staged vulnerabilities which when solved present a key for scoring/reporting that it was discovered.

In the same vein, this CTF challenge will also leverage the ICS Village’s ICS Ranges including physical and virtual environments to provide an additional testbed for more advanced challenges in critical infrastructure and ICS environments. New this year, there will be integrated elements from DHS/CISA with their newly built mobile environments that are realistically miniaturized assets (ie - operational oil and natural gas pipeline, etc.) and will be the first they’ll be opened to the public for hacking.

Forum: <https://forum.defcon.org/node/233029>

Discord: <https://discord.com/channels/708208267699945503/711643691877531698>

Twitter: https://twitter.com/ICS_Village

Web: <https://www.icsvillage.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ICS Hack the Plan[e]t

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Hack the Plan[e]t Capture the Flag (CTF) contest will feature Howdy Neighbor and the Industrial Control System (ICS) Range. This first of its kind CTF will integrate both Internet of Things (IoT) and ICS environments with interactive components for competitors to test their skills and knowledge.

Howdy Neighbor is an interactive IoT CTF challenge where competitors can test their hacking skills and learn about common oversights made in development, configuration, and setup of IoT devices. Howdy Neighbor is a miniature home - made to be “smart” from basement to garage. It’s a test-bed for reverse engineering and hacking distinct consumer-focused smart devices, and to understand how the (in)security of individual devices can implicate the safety of your home or office, and ultimately your family or business. Within Howdy Neighbor there are over 25 emulated or real devices and over 50 vulnerabilities that have been staged as challenges. Each of the challenges are of varying levels to test a competitors ability to find vulnerabilities in an IoT environment. Howdy Neighbor’s challenges are composed of a real or simulated devices controlled by an App or Network interface and additional hardware sensors; each Howdy Neighbor device contains 1 to 3 staged vulnerabilities which when solved present a key for scoring/reporting that it was discovered.

In the same vein, this CTF challenge will also leverage the ICS Village’s ICS Ranges including physical and virtual environments to provide an additional testbed for more advanced challenges in critical infrastructure and ICS environments. New this year, there will be integrated elements from DHS/CISA with their newly built mobile environments that are realistically miniaturized assets (ie - operational oil and natural gas pipeline, etc.) and will be the first they’ll be opened to the public for hacking.

Forum: <https://forum.defcon.org/node/233029>

Discord: <https://discord.com/channels/708208267699945503/711643691877531698>

Twitter: https://twitter.com/ICS_Village

Web: <https://www.icsvillage.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ICS Hack the Plan[e]t

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Hack the Plan[e]t Capture the Flag (CTF) contest will feature Howdy Neighbor and the Industrial Control System (ICS) Range. This first of its kind CTF will integrate both Internet of Things (IoT) and ICS environments with interactive components for competitors to test their skills and knowledge.

Howdy Neighbor is an interactive IoT CTF challenge where competitors can test their hacking skills and learn about common oversights made in development, configuration, and setup of IoT devices. Howdy Neighbor is a miniature home - made to be “smart” from basement to garage. It’s a test-bed for reverse engineering and hacking distinct consumer-focused smart devices, and to understand how the (in)security of individual devices can implicate the safety of your home or office, and ultimately your family or business. Within Howdy Neighbor there are over 25 emulated or real devices and over 50 vulnerabilities that have been staged as challenges. Each of the challenges are of varying levels to test a competitors ability to find vulnerabilities in an IoT environment. Howdy Neighbor’s challenges are composed of a real or simulated devices controlled by an App or Network interface and additional hardware sensors; each Howdy Neighbor device contains 1 to 3 staged vulnerabilities which when solved present a key for scoring/reporting that it was discovered.

In the same vein, this CTF challenge will also leverage the ICS Village’s ICS Ranges including physical and virtual environments to provide an additional testbed for more advanced challenges in critical infrastructure and ICS environments. New this year, there will be integrated elements from DHS/CISA with their newly built mobile environments that are realistically miniaturized assets (ie - operational oil and natural gas pipeline, etc.) and will be the first they’ll be opened to the public for hacking.

Forum: <https://forum.defcon.org/node/233029>

Discord: <https://discord.com/channels/708208267699945503/711643691877531698>

Twitter: https://twitter.com/ICS_Village

Web: <https://www.icsvillage.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Friday - 10:15-10:45 PDT

Title: ICS Village CTF Kick-Off

When: Friday, Aug 7, 10:15 - 10:45 PDT

Where: ICS Vlg

SpeakerBio: Tom

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Saturday - 13:30-13:59 PDT

Title: Identifying and fixing out-of-gas errors in smart contracts with smart fuzzing

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: Blockchain VIg

SpeakerBio: Sebastian Banescu

No BIO available

Description: No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Identity Crisis: the mad rise of online account opening fraud

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Payment Vlg

SpeakerBio: Uri Rivner

No BIO available

Description:

Identity data is a commodity these days, and conducting identity theft or synthetic ID operations has never been easier. In this 100% real case study we'll track the second-by-second operation of cyber criminals attempting to target major card issuers and digital banks.

We'll discuss their behavior, choices and motivations, what makes them so different than honest folks who wish to open an account online, and what next-gen data sources and analysis domains the industry is beginning to leverage against such attacks. It's time to put up a good fight!

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ILS and TCAS Spoofing Demonstration

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: Aerospace Vlg

SpeakerBio: Alex Lomas

Alex Lomas is Pen Test Partner's aerospace specialist. Alex undertakes penetration testing of traditional IT, such as networks, web applications, and APIs, as well as more aviation-specific areas including airport operational technology and avionics embedded systems such as inflight entertainment and e-enabled aircraft.

Description:

The Traffic Alert & Collision Avoidance System or TCAS was first developed in the early 1980s using transponders on aircraft to interrogate other aircraft within a set range about their distance, altitude, and heading. If a collision course is detected and the aircraft is suitably equipped, a TCAS alert will be sounded. In certain autopilot modes (mostly on Airbus), the aircraft will automatically follow the TCAS Resolution Advisory and climb or descend with no input from the pilot. Others have shown that it's possible to create fake TCAS traffic. We've taken this further and investigated how airplanes equipped with autopilots capable of flying a resolution advisory themselves would respond in certain scenarios.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Sunday - 13:00-13:59 PDT

Title: Importing vector graphics in to EagleCAD

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: Hardware Hacking Vlg

Description:

Twitch: <https://www.twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOT - Saturday - 13:45-14:15 PDT

Title: In search of the perfect UPnP tool

When: Saturday, Aug 8, 13:45 - 14:15 PDT

Where: IOT VIg

SpeakerBio: Trevor Stevado t1v0

Trevor is the Founding Partner of Loudmouth Security, an elite penetration testing and red teaming company in Canada's National Capital. Trevor has a black badge from DefCon 26 and is co-organizer for IoT Village at conferences across the Canada and the US.

Twitter: [@_t1v0_](https://twitter.com/_t1v0_)

Description:

While researching UPnP vulnerabilities I became frustrated with the currently available UPnP tools. Some devices that I knew had UPnP just weren't found with any of the tools I tried. Out of this frustration, came a new and improved BHunter extension for Burp Suite. In this lightning talk I'll go over some of the issues I found and the improvements made to it, and I'll give a demo of the tool in action.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CRV - Friday - 15:00-15:59 PDT

Title: In theory, there is no difference between theory and practice

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: Career Hacking VIg

SpeakerBio: Pablo Breuer

No BIO available

Description:

There are three general paths to an INFOSEC career: the school of hard knocks, certificates, and college. Every few months a flame war erupts out arguing which is the "right" path. What are the pros and cons of each of these paths? Come have a balanced conversation about the three paths and learn which is the best one for you depending upon your unique needs

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Incident Response and the ATT&CK Matrix (Beginner)

When: Sunday, Aug 9, 10:30 - 11:59 PDT

Where: Blue Team VIg - Workshop Track 2

SpeakerBio: Sam Bowne , Founder, Infosec Decoded Inc.; Instructor, 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

Twitter: [@sambowne](https://twitter.com/sambowne)

Description:

Practice techniques to detect, analyze and respond to intrusions on cloud servers. We will emulate APT attacks and detect them with Splunk, Suricata, Sysmon, Wireshark, Yara and other tools. We will use the ATT&CK Matrix to enumerate threat actors, tactics and techniques.

Beginners are welcome. No previous experience with these techniques is required. Participants need a credit card and a few dollars to rent Google Cloud servers.

Practice techniques to detect, analyze and respond to intrusions. We will construct targets and attackers on the Google cloud, and send attacks using Metasploit and Caldera to emulate APT attackers. We will monitor and analyze the attacks using Splunk, Suricata, Sysmon, Wireshark, Yara and online analysis tools including PacketTotal and VirusTotal.

We will cover the ATT&CK Matrix in detail, which enumerates threat actors, tactics and techniques, so red and blue teams can better communicate and work together to secure networks.

The workshop is structured in a CTF format. Each participant works at their own pace. The techniques will be demonstrated, with complete step-by-step instructions to lead beginners through the easy challenges. There are also harder challenges for more experienced participants. We will help participants as needed, to ensure that everyone learns new techniques.

Participants need a credit card and a few dollars to rent Google Cloud servers. We will use Debian Linux and Windows Server 2016 systems. All the tools we will use are freely available, and all the training materials will remain available to everyone after the workshop ends.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Incident Response Panel

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: Blue Team Vlg - Talks Track 1

Speakers: Russell Mosley, Vyrus, Litmoose, Xavier Ashe

SpeakerBio: Russell Mosley

Russell is a 'hands-on' CISO who 'still knows how to use tcpdump' with over 20 years experience in systems administration, secops, audits and compliance. Russell is an volunteer with several Bsidess events and the Blue Team Village, who prefers turning wrenches and crashing drones in his spare time.

Twitter: [@sm0kem](#)

SpeakerBio: Vyrus

No BIO available

Twitter: [@vyrus001](#)

SpeakerBio: Litmoose

No BIO available

Twitter: [@LitMoose](#)

SpeakerBio: Xavier Ashe

No BIO available

Description:

Our panel of experts will discuss lessons learned from their experiences on the front lines of incident response. What happens during a breach? What are common mistakes victims make? What are key steps you can take to prepare for the worst? How can you best secure your organization today?

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Indicators of Emulation (Intermediate)

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio:Ch33r10

@ch33r10 works for a Financial Services Fortune 500 Company. She is a graduate of the SANS 2017 Women's Academy, has an MBA in IT Management, and currently holds the GSEC, GCIH, GCFE, GMON, GDAT, GPEN and GCTI certifications. She is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), Yara Exchange, and FuzzySnugglyDuck. @ch33r10 is a doctoral student at Marymount University and has served on multiple CFP review boards.

Twitter: [@ch33r10](#)

Description:

Cyber threat intelligence, in the past, has primarily focused on extracting, preparing, and analyzing indicators of compromise for digital forensics and incident response, the security operations center, and other teams. This talk proposes that cyber threat intelligence analysts extract indicators of emulation and include them in their threat reports for red team operations, adversary emulation, and purple team exercises. Learn how to extract Indicators of Emulation in Windows-based malware for high-value adversary emulation and purple team exercises based upon org specific data.

Cyber threat intelligence plays a pivotal role in collecting and analyzing data to produce intelligence for an organization. Most of the cyber threat intelligence reports include indicators of compromise that various teams, such as incident response, hunt, and security operations, consume; however, there is limited intelligence in most threat reports geared towards adversary emulation. There is a lack of research or information regarding indicators related to emulating an attacker's malware, mainly Windows-based malware. As cyber threat intel teams mature through using their internal attack data to produce intelligence, it becomes necessary to determine how to build out existing capabilities and provide additional value to other teams in the organization. Cyber threat intelligence analysts can contribute to adversary emulation exercises through extracting indicators of emulation to include in their threat intelligence reports for a realistic emulation of the adversary. Here's what I plan on showing the audience how to do step-by-step and with a pre-recorded demo: -Audit Log setup for Win10 VM -Disable Window Defender SmartScreen before downloading samples -Create custom "test malware to ensure command-line Audit logging is set up properly (blue teamers popping calc with a custom compiled program made in C++). -walk through how I picked samples from URLhaus so they can practice at home or use their own org's samples -walk through of what I looked for in the command-line -Discussion of where I am at in the research -Ideas/suggestions on how to package the Indicators of Emulation for Adversary Emulation, Red Teams, and Purple Exercises. ***I will document everything very well and include it in my presentation as a resource. I only need 15 minutes.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Indicators of Emulation: Extra Spicy Adversary Emulation

When: Saturday, Aug 8, 16:30 - 17:30 PDT

Where: Red Team VIg

Speakers:Ch33r10,haydnjohnson

SpeakerBio:Ch33r10

@ch33r10 works for a Financial Services Fortune 500 Company. She is a graduate of the SANS 2017 Women's Academy, has an MBA in IT Management, and currently holds the GSEC, GCIH, GCFE, GMON, GDAT, GPEN and GCTI certifications. She is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), Yara Exchange, and FuzzySnugglyDuck. @ch33r10 is a doctoral student at Marymount University and has served on multiple CFP review boards.

Twitter: [@ch33r10](#)

SpeakerBio:haydnjohnson

@haydnjohnson has over 7 years of information security experience, including network/web penetration testing, vulnerability assessments and Cyber Threat Intelligence. He was on the 2019 SANS Purple Team CFP review board and currently holds the OSCP, GXPN and eCIR certifications. @haydnjohnson has gained both red and blue team experience.

Twitter: [@haydnjohnson](#)

Description:

Cyber threat intelligence, in the past, has primarily focused on extracting, preparing, and analyzing indicators of compromise for digital forensics and incident response, the security operations center, and other teams. This talk proposes that there is a benefit to including cyber threat intelligence analysts in adversarial threat emulation. By including indicators of emulation (IOE) based upon internal organizational attack data, CTI analysts can enrich and customize red team TTPs to specific threats the organization is currently facing. Don't have a CTI team? Well, we have solutions for you! From pulling TTPs and IOEs out of thin air to a custom Golang C2 tool you can use to execute payloads that are relevant to your organization. Sit back, relax, and enjoy the show!

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Saturday - 16:45-17:15 PDT

Title: Industrial Cybersecurity in Mexico

When: Saturday, Aug 8, 16:45 - 17:15 PDT

Where: ICS Vlg

Speakers: Octavio Fernandez, Victor Gomez

SpeakerBio: Octavio Fernandez

No BIO available

SpeakerBio: Victor Gomez

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Infodemic: Threat models for patient communities on social networks

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: BioHacking Vlg

SpeakerBio: Andrea Downing

Andrea Downing is a Community Data Organizer, security researcher, and advocate hereditary cancer community. In 2018, she discovered the a security vulnerability that affected all closed groups on Facebook. She served on the organizing team at Stanford Medicine X.

Description:

People going through trauma are more vulnerable to misinformation. First coined by the World Health Organization, COVID19 has sparked a widespread infodemic. This talk will examine examples of disinformation campaigns. We'll look at ways that sock puppets target, scrape, at spread misinformation on COVID. Finally, we'll look at some examples of how disinformation has caused harm and loss of life for vulnerable populations.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Initial Compromise through Web Side

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: Red Team VIg

SpeakerBio: Walter Cuestas

Walter Cuestas - Pentester and Red Teamer for Open-Sec LLC and Cobalt Labs Inc with more then 15 years of experience focused on infrastructure and web applications pentesting and red team operations. Speaker at Ekoparty (several years) and instructor at DEF CON 26 (Lateral Movement workshop).

Description:

Initial compromise seems to be tied to client side, but, there are several attack vectors on Web side besides a simple RCE. During this talk I will show 3 cases of getting the initial compromise through vulnerabilities found in application servers and thin clients services going from breaking authentication process, escaping controls and how to solve some challenges during exploitation of what seems an easy peasy. Objectives of this talk are : show how important is to make a good OSINT, make a good dictionary, manage escape sequences in thin client services, how to modify already developed exploits for our current target and the benefit for blue teams to have applications security integrated with infrastructure/operations security.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Inside the Mind of a Threat Actor: Beyond Pentesting

When: Saturday, Aug 8, 12:15 - 12:30 PDT

Where: Red Team VIg

SpeakerBio: Phillip Wylie

Phillip Wylie is the Senior Red Team Lead for a global consumer products company, Adjunct Instructor at Richland College, and The Pwn School Project founder. Phillip has over 22 years of experience with the last 8 years spent as a pentester. Phillip has a passion for mentoring and education. His passion motivated him to start teaching and founding The Pwn School Project a monthly educational meetup focusing on cybersecurity and ethical hacking. Phillip teaches Ethical Hacking and Web Application Pentesting at Richland College in Dallas, TX. Phillip is a co-host for The Uncommon Journey podcast. Phillip holds the following certifications; CISSP, NSA-IAM, OSCP, GWAPT.

Description:

Red team is a commonly misunderstood offensive security discipline. Red team has been used as a general term for all areas of offensive security just as blue team for defensive security. True red teaming goes Beyond Pentesting and into more adversarial emulation. While there are overlapping skills, there are differences that will be discussed as Phillip shares his experience of going from a pentester to a red teamer. In this talk, you will learn about the different areas that make up red team operations, common tools, and the path to becoming a red teamer. In this presentation, you will learn about resources helpful for a path into red teaming.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCG - Saturday - 15:00-15:15 PDT

Title: Intro to DC603

When: Saturday, Aug 8, 15:00 - 15:15 PDT

Where: DEF CON Groups

Description:

Presentation by DC603 (New Hampshire, USA)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

DCG - Saturday - 13:00-13:15 PDT

Title: Intro to DC858

When: Saturday, Aug 8, 13:00 - 13:15 PDT

Where: DEF CON Groups

Description:

Presentation by DC858 (San Diego, California, USA)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

LPV - Saturday - 17:00-17:59 PDT

Title: Intro to high security locks and lockpicking

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: Lockpick Vlg

SpeakerBio:N thing

No BIO available

Description:

This is a quick introduction to high security locks, what they are, what they look like and how to get started defeating them.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 10:00-10:30 PDT

Title: Intro to Lockpicking

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 12:00-12:30 PDT

Title: Intro to Lockpicking

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 14:15-14:45 PDT

Title: Intro to Lockpicking

When: Friday, Aug 7, 14:15 - 14:45 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 16:15-16:45 PDT

Title: Intro to Lockpicking

When: Friday, Aug 7, 16:15 - 16:45 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Saturday - 10:00-10:30 PDT

Title: Intro to Lockpicking

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Intro to Lockpicking

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Intro to Lockpicking

When: Saturday, Aug 8, 14:15 - 14:45 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Intro to Lockpicking

When: Saturday, Aug 8, 16:15 - 16:45 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 10:00-10:30 PDT

Title: Intro to Lockpicking

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 12:00-12:30 PDT

Title: Intro to Lockpicking

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 14:15-14:45 PDT

Title: Intro to Lockpicking

When: Sunday, Aug 9, 14:15 - 14:45 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Sunday - 16:15-16:45 PDT

Title: Intro to Lockpicking

When: Sunday, Aug 9, 16:15 - 16:45 PDT

Where: Lockpick Vlg

SpeakerBio: The Open Organisation Of Lockpickers

No BIO available

Twitter: [@toool](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Introducing DropEngine: A Malleable Payload Creation Framework

When: Thursday, Aug 6, 15:30 - 16:30 PDT

Where: Red Team VIg

SpeakerBio: Gabriel Ryan

Gabriel Ryan is an offensive security engineer at SpecterOps with nearly 8 years of programming experience in C and Python. Previously, he worked at Gotham Digital Science, where he was heavily involved in their research program GDS Labs. He is the creator and active developer of EAPHammer, a weaponized version of hostapd for performing rogue access point attacks against WPA/2-EAP networks. He is also credited with the first working bypass of 802.1x-2010, along with improvements to existing techniques for bypassing 802.1x-2004. Gabriel's most recent research involved novel proof-of-concept attacks against WPA3's "Enhanced Open." His current endeavors involve deep dives into Kerberos abuse on both Windows and Linux platforms.

Description:

In this talk, we'll introduce DropEngine -- a modular framework for creating malleable initial access payloads (also known as "droppers" or "shellcode runners").

Initial access payloads serve a deceptively simple purpose: loading implants from disk into memory. However, a number of obstacles stand in the way of this seemingly mundane task. To start with, the payload must safely be delivered to its intended target (usually via spearphishing). During delivery, the payload is exposed to signature-based detections and analyzed from within an automated sandbox. The payload must then be saved to disk without triggering antivirus, and must load the implant into memory without alerting Endpoint Detection and Response (EDR). Due to the widespread use of application whitelisting, payload authors are restricted to languages that are compatible with "Live Off the Land Binaries and Scripts" (LOLBAS), most of which are executed through the Windows Common Language Runtime (CLR). This means that most payloads must also contend with Microsoft's Anti-Malware Scan Interface (AMSI). Finally, the payload must be able to withstand analysis by threat hunters and reverse engineers. These obstacles are not insurmountable. However, defense evasion techniques tend to have a short shelf-life, and become particularly stale after repeated use. Because of this, payloads are often prepared on a per-engagement basis, which is hardly an easy feat when done by hand. DropEngine addresses this problem by providing a malleable framework for creating shellcode runners. Operators can choose from a selection of components and combine them to create highly sophisticated payloads within seconds. Available payload components include crypters, execution mechanisms, and environmental and remote keying functions. Also included are pre-execution modules such as sandbox checks and AMSI bypasses, as well cleanup modules that execute after the implant is loaded into memory. DropEngine comes pre-packaged with example modules that are more than sufficient to bypass signature and heuristic-based detections at the time of writing. However, DropEngine's true strength is that it improves operational efficiency by providing a high degree standardization, while allowing operators to control just about every aspect of the payload's signature and behavior.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCG - Saturday - 17:00-17:59 PDT

Title: Introducing Melbourne DCG by Allen and Friends

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: DEF CON Groups

Description:

Presentation by DCG11613 (Melbourne, Australia)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Introducing the Meet a Mentor Program

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: Blue Team VIg - Talks Track 1

Speakers:Scoubi,Plug,Litmoose,Xavier Ashe,Rand0h,Muteki,PacketSqueezins,ttheveii0x,Allie Hansen,nohackme

SpeakerBio:Scoubi

Mathieu Saulnier is a “Security Enthusiast @h3xstream. He has held numerous positions as a consultant within several of Quebec’s largest institutions. For the last 8 years he has been focused on putting in place a few SOC and has specialized in detection (Blue Team), content creation and mentorship. He worked as a † Senior Security Architect » and acted as “Adversary Detection Team Lead and “Threat Hunting Team Lead for one of Canada’s largest carrier for many years and is now SOC Team Lead in a large financial institution. He loves to give talk and had the honor to do so at GoSec, BSidesCharm, NorthSec, BSidesLV, Defcon’s BTV and Derbycon.

Twitter: [@ScoubiMtl](#)

SpeakerBio:Plug

No BIO available

Twitter: [@plugxor](#)

SpeakerBio:Litmoose

No BIO available

Twitter: [@LitMoose](#)

SpeakerBio:Xavier Ashe

No BIO available

SpeakerBio:Rand0h

No BIO available

SpeakerBio:Muteki

No BIO available

SpeakerBio:PacketSqueezins

Garrett's career started in systems administration, took a couple detours, jumped to Big 4 advisory security consulting and penetration testing, eventually landed in boutique security consulting @secrisk. Specializes in solving weird and seemingly impossible problems.

Organizer for BSides Philly (badges), builds trebuchets for fun (Punkin Chunkin, when it was still a thing) among other things.

Twitter: [@LegitBinary](#)

SpeakerBio:ttheveii0x

No BIO available

SpeakerBio:Allie Hansen

No BIO available

SpeakerBio:nohackme

Mick fell in love with the idea of cyberspace around 9 years old after reading Neuromancer, which led him to pursue a career

in computer operations, with a focus on information security. He was the Chief Information Security Officer at Pete for America; holding the honor of being the first CISO in the history of presidential campaigns. Previously the White House Threat Intelligence Branch Chief in both the Obama and Trump administrations, Mick also helped create a threat intelligence program during the rollout of the Affordable Care Act at the Department of Health and Human Services. Mick has served in cybersecurity and technical roles at the Department of Defense and Centers for Disease Control, and is a US Navy veteran. Mick is currently a Security Advisor at Splunk, leveraging his background and expertise to help customers solve security problems. When not posting pictures of cats, food, and sneakers to social media, Mick is the Vice President of The Open Organisation of Lockpickers in Washington DC, and a SOC Goon at DEFCon.

Twitter: [@nohackme](https://twitter.com/nohackme)

Description:No Description available

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Introduction To ACARS

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: Aerospace VIg

SpeakerBio: Alex Lomas

Alex Lomas is Pen Test Partner's aerospace specialist. Alex undertakes penetration testing of traditional IT, such as networks, web applications, and APIs, as well as more aviation-specific areas including airport operational technology and avionics embedded systems such as inflight entertainment and e-enabled aircraft.

Description:

We'll go through what ACARS is, its roots in Telex, through to how it's implemented and used in modern airline operations today over VHF, HF, and SATCOM.

We'll talk about how to setup your own ACARS receiver using an RTL-SDR and do a live demo of capturing real ACARS transmissions and attempt to decode what those messages are about. Then we'll take a thought experiment on how potentially malicious transmissions could be made to affect the aircraft.

There will also be a discussion around how ACARS is used in modern CPDLC air traffic to pilot data links, instead of voice communications and how these could be vulnerable, and a brief look at SELCAL which reduces the need for pilots to monitor the radio.

Lastly we'll look at the future of ACARS over IP and how this will integrate with modern e-enabled aircraft.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Introduction to Malware Analysis & Response (MA&R) (Beginner)

When: Sunday, Aug 9, 09:00 - 10:30 PDT

Where: Blue Team Vlg - Workshop Track 1

SpeakerBio: Michael Wylie, Director of Cybersecurity Services, Richey May Technology Solution
Michael Wylie (Twitter: @TheMikeWylie), MBA, CISSP is the Director of Cybersecurity Services at Richey May Technology Solutions. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, cloud security, penetration tests, risk management, and training. Michael has developed and taught numerous courses for the U.S. Department of Defense, DEFCON, Universities, and for clients around the world. Michael is the winner of numerous SANS challenge coins and holds the following credentials: CISSP, CCNA R&S, CCNA CyberOps, GMON, GPEN, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, Security+, Project+, and more.
Twitter: @TheMikeWylie

Description:

In this introductory hands-on fundamental malware analysis workshop. IT and Cybersecurity professionals will learn the basic skills necessary to safely analyze the characteristics and behavior of malware. Students will walk away with practical techniques and methodologies that can be immediately applied to statically and dynamically analyzing software with an emphasis on malicious software. Gone are the days where incident responders reformat infected systems destroying valuable evidence. Preserving and analyzing malware artifacts will give attendees the skills to understand, at a high level, the techniques and malicious intents of malware that defeated their security controls.

LEARNING OBJECTIVES

1. Understand fundamentals of malware analysis
2. Understand the goals and benefits of performing malware analysis
3. Be able to perform basic static analysis on Windows malware
4. Be able to setup a malware analysis lab
5. Be able to perform dynamic analysis on Windows malware

Who should take this course?

IT and Cybersecurity students and professionals. This is an introduction to malware analysis course for beginners.

What will students be provided with?

Students will be provided with a Windows 10 virtual machines (trial version) with malware analysis tools and training material. Attendees will be provided with step-by-step instructional labs.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOT - Saturday - 11:00-11:59 PDT

Title: Introduction to U-Boot Interaction and Hacking

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: IOT VIg

SpeakerBio:Garrett Enoch

No BIO available

Description:

This learning session will guide the attendees through various concepts related U-boot including hacks to gain access to U-boot console, U-boot console commands and structure and various methods on using U-boot to exploit an embedded IoT systems. After each learning objective we will have Q&A sessions.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Introduction to WiFi Security

When: Thursday, Aug 6, 09:00 - 09:01 PDT

Where: Wireless Vlg

SpeakerBio: Nishant Sharma , R&D Manager, Pentester Academy

Nishant Sharma (Twitter: @wifisecguy) is an R&D Manager at Pentester Academy and Attack Defense. He is also the Architect at Hacker Arsenal where he leads the development of multiple gadgets for WiFi pentesting such as WiMonitor, WiNX and WiMini. He also handles technical content creation and moderation for Pentester Academy TV. He has 7+ years of experience in information security field including 5+ years in WiFi security research and development. He has presented/published his work at Blackhat USA/Asia, DEF CON China, Wireless Village, IoT village and Demo labs (DEFCON USA). Prior to joining Pentester Academy, he worked as a firmware developer at Mojo Networks where he contributed in developing new features for the enterprise-grade WiFi APs and maintaining the state of art WiFi Intrusion Prevention System (WIPS). He has a Master's degree in Information Security from IIIT Delhi. He has also published peer-reviewed academic research on HMAC security. His areas of interest include WiFi and IoT security, AD security, Forensics and Cryptography.

Twitter: [@wifisecguy](https://twitter.com/wifisecguy)

Description:

Every year a lot of new people attend DEF CON to explore new topics and some even move to new fields based on their newly discovered interests. The workshops organised by the DEF CON villages always played an important role. This year the DEF CON has gone virtual and it is apt for the workshops to do so too.

Our workshop is focused on the beginner people who want to explore/learn WiFi security and understand how the WiFi network attacks work. To adapt to this new normal, we will change the approach a little, we will explain the basics and theory (in brief) using slides and then give the users access to our cloud labs. The labs consist of an emulated WiFi environment and the users have everything they need to get cracking along with step by step instructions. We are planning to cover the following:

- Basics of WiFi (What is WiFi, important standard, bands, channels, SSID, BSSID)
- Introduction to WiFi Recon (Locating nearby APs and clients)

-WEP (What is WEP, How it works, Why WEP is broken, How to hack WEP)

-WPA2-PSK (What is WPA2-PSK, How 4-way handshake works, How to crack WPA2-PSK)

-WPA2-ENT (What is WPA2-ENT, How MSCHAPv2 auth works, How to crack WPA2-ENT MSCHAPv2)

This talk is available on YouTube.

Link from instructor: <http://linux-basics-bootcamp-pa-beta.ue.r.appspot.com/courses/>

Talk: https://www.youtube.com/watch?v=zV_yWVTbhlc

Return to Index - Add to  - ics [Calendar](#) file

Title: Intrusion Analysis and Threat Hunting with Open Source Tools

When: Friday, Aug 7, 13:00 - 14:59 PDT

Where: Packet Hacking Vlg - Workshop

Speakers: Jack Mott, Jason Williams, Josh Stroschein

SpeakerBio: Jack Mott , Security Researcher

Jack Mott is a security researcher who focuses on open source solutions to detect, track and hunt malware and malicious activity. He has been a signature writer for the Emerging Threats team for several years, producing community/premium Suricata signatures to help protect networks worldwide. Jack is a strong believer in the open source mission as well as helping people and organizations solve security issues with open source solutions. He resides in the USA.

SpeakerBio: Jason Williams , Security Researcher

Jason Williams is a security researcher with global enterprise experience in detecting, hunting and remediating threats with open source technologies. Primarily focusing on network communications, Jason has written thousands of commercial and community Suricata rules for Emerging Threats to help defenders protect their networks. Jason participates as a Signature Development and User Training instructor for the OISF.

SpeakerBio: Josh Stroschein , Director of Training, Open Information Security Foundation (OISF) / Suricata

Josh Stroschein is an experienced malware analyst and reverse engineer who has a passion for sharing his knowledge with others. He is the Director of Training for OISF, where he leads all training activities for the foundation and is also responsible for academic outreach and developing research initiatives. Josh is an accomplished trainer, providing training in the aforementioned subject areas at BlackHat, DerbyCon, Toorcon, Hack-In-The-Box, Suricon and other public and private venues. Josh is an Assistant Professor of Cyber Security at Dakota State University where he teaches malware analysis and reverse engineering, an author on Pluralsight, and a threat researcher for Bromium.

Description:

In today's threat landscape, sophisticated adversaries have routinely demonstrated the ability to compromise enterprise networks and remain hidden for extended periods of time. In Intrusion Analysis and Threat Hunting with Open Source Tools, you will learn how to dig deep into network traffic to identify key evidence that a compromise has occurred, learn how to deal with new forms of attack, and develop the skills necessary to proactively search for evidence of new breaches. We will explore key phases of adversary tactics and techniques - from delivery mechanisms to post-infection traffic to get hands-on analysis experience. Open-source tools such as Suricata and Moloch will be utilized to generate data, perform exhaustive traffic analysis, and develop comprehensive threat hunting strategies. By the end of this workshop, you will have the knowledge and skills necessary to discover new threats in your network.

This workshop requires registration. If you are registered, please proceed to #phv-infobooth-text and you'll be given access to join.

#phv-infobooth-text: <https://discord.com/channels/708208267699945503/708242376883306526>

Return to Index - Add to  - ics [Calendar](#) file

Title: IoT Hacking Stories in Real Life

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: IOT Vlg

SpeakerBio: Besim Altinok

Besim Altinok (@AltnokBesim) has been researching Wi-Fi security for over a decade. He created WiPi-Hunter project against Wi-Fi hackers. He is the author of a book on Wi-Fi security. Besim's work on wireless security has been published in ArkaKapi Magazine and others. He has also spoken at top conferences including BlackHat Europe, Blackhat ASIA, Defcon, and others. Besim ALTINOK works currently at a Private Company which is located in Ankara, Turkey

Twitter: [@AltnokBesim](#)

Description:

Throughout this year, we had the chance to analyze two different models of electric scooters, three different models of smart locks, various kind of smart home devices and lastly one robot assistant which is in use at airports. During the analysis process, we have found some critical security vulnerabilities including privilege escalation, insecure communication and taking over the servers which these communications are being performed on. Additionally, we have identified two hard-coded secret keys and lastly one cryptographic key in the result of our analysis. In this presentation, we will be sharing the details of the vulnerabilities that we have identified during our analysis.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOT - Saturday - 17:00-17:45 PDT

Title: IoT Honeypots and taming Rogue appliances

When: Saturday, Aug 8, 17:00 - 17:45 PDT

Where: IOT VIg

SpeakerBio: Kat Fitzgerald

Based in Pittsburgh and a natural creature of winter, you can typically find me sipping Grand Mayan Extra Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos. Honeypots & Refrigerators are a few of my favorite things! Fun Fact: I rescue Feral Pop Tarts and have the only Pop Tart Sanctuary in the Pittsburgh area.

Description:

Honeypots AND IoT security, all in one place? Yes, why YES I tell you, and this is it! Oh sure, honeypots are not new, but how they are used is what makes this talk just a little bit different. Presented for your viewing pleasure will be IoT specific honeypot configurations, some deployed with k8s (some not) and how they are used to not only trap attacks against your IoT devices but also detect attacks FROM a compromised IoT device.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: IoT Under the Microscope: Vulnerability Trends in the Supply Chain

When: Friday, Aug 7, 13:15 - 13:59 PDT

Where: IOT VIg

SpeakerBio: Parker Wiksell

Parker Wiksell (@pwiksell) is a security researcher and engineer at Finite State, an IoT security research company, and is the author of the AFL-Unicorn fuzzer and the Patchwerk kernel patching framework. Parker has over 25 years industry experience, with the last 9 being focused primarily on software and hardware security research, presenting at several major conferences. When not geeking out on computers, Parker has been known to write the occasional musical composition professionally.

Twitter: [@pwiksell](#)

Description:

IoT device manufacturers have no idea what's running on their devices -- they really don't.

In 2002 then-US Secretary of Defense, Donald Rumsfeld, brought public attention to a notion that information can be divided into three categories: known knowns, known unknowns, and unknown unknowns. As hackers, how can we apply this formulation to IoT vulnerabilities?

The known knowns: Vulnerabilities that have been explicitly discovered through scanning and testing. The known unknowns: Newly created software that has yet to undergo any application security testing. The unknown unknowns: Systems that the defender does not know about.

There is, in fact, a fourth dimension: unknown knowns, which comprise “that which we intentionally refuse to acknowledge that we know” or “do not like to know. The unknown knowns: Vulnerabilities that are known to exist, but that have not been associated with all the systems they actually affect.

In this talk, we report on IoT device vulnerability findings at massive scale, as a result of our firmware collection and analysis. For this research we have selected approximately 50k firmware images, representing over 7M files, 10k products, and 150 vendors, spanning many different architectures and operating systems. We will highlight some of the trends we've uncovered in supply chain vulnerabilities, and reveal specific examples of device backdoors, botnets, and vulnerabilities discovered in medical, home, and commercial device firmware.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: jeopardize

When: Saturday, Aug 8, 10:00 - 11:50 PDT

Where: See Description or Village

SpeakerBio: Utku Sen

Utku Sen is a security researcher who is mostly focused on application security, network security and tool development. He presented his different tools and researches in Black Hat USA Arsenal, DEF CON Demo Labs, Packet Hacking Village and Recon Village in the recent years. He's also nominated for Pwnie Awards on "Best Backdoor" category in 2016. He is currently working for HackerOne.

Description:

Jeopardize tool is developed to provide basic threat intelligence&response capabilities against phishing domains at the minimum cost as possible. It detects registered phishing domain candidates (typosquatting, homograph etc.), analyzes them and assigns a risk score to them. After then, it sends valid-looking credentials to the login forms on those phishing sites. Main goals are to confuse the attackers and to buy organizations some time to take precautions.

Audience: Defense

Discord: #dl-sen-jeopardize-text: <https://discord.com/channels/708208267699945503/730256291032989728>

Watch @ #dl-video2-voice: <https://discord.com/channels/708208267699945503/734027778646867988>

Github: <https://github.com/utkusen/jeopardize>

Forum: <https://forum.defcon.org/node/233129>

Return to Index - Add to  - ics [Calendar](#) file

Title: jeopardyize

When: Friday, Aug 7, 14:00 - 15:50 PDT

Where: See Description or Village

SpeakerBio: Utku Sen

Utku Sen is a security researcher who is mostly focused on application security, network security and tool development. He presented his different tools and researches in Black Hat USA Arsenal, DEF CON Demo Labs, Packet Hacking Village and Recon Village in the recent years. He's also nominated for Pwnie Awards on "Best Backdoor" category in 2016. He is currently working for HackerOne.

Description:

Jeopardize tool is developed to provide basic threat intelligence&response capabilities against phishing domains at the minimum cost as possible. It detects registered phishing domain candidates (typosquatting, homograph etc.), analyzes them and assigns a risk score to them. After then, it sends valid-looking credentials to the login forms on those phishing sites. Main goals are to confuse the attackers and to buy organizations some time to take precautions.

Audience: Defense

Discord: #dl-sen-jeopardize-text: <https://discord.com/channels/708208267699945503/730256291032989728>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://github.com/utkusen/jeopardize>

Forum: <https://forum.defcon.org/node/233129>

Return to Index - Add to  - ics [Calendar](#) file

VMV - Saturday - 10:30-10:59 PDT

Title: John Odum, Montpelier, VT

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: Voting Vlg

SpeakerBio: John Odum , City Clerk, Montpelier, Vermont
CMC, CEH, CNDA, MCP, CIW

Description: No Description available

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar file](#)

AIV - Saturday - 13:00-13:59 PDT

Title: Journal Club Live! Fawkes FR

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: AI Vlg

SpeakerBio: AI Village Journal Club

No BIO available

Description: No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: JWT Parkour

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: AppSec Vlg

SpeakerBio: Louis Nyffenegger

No BIO available

Twitter: [@snyff](#)

Description:

Nowadays, JSON Web Tokens are everywhere. They are used as session tokens or just to pass data between applications or services. By design, JWT contains a high number of security and cryptography pitfalls. In this workshop, we are going to learn how to exploit some of those issues!

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Friday - 11:00-11:50 PDT

Title: Key Duplication - It's not just for the movies!

When: Friday, Aug 7, 11:00 - 11:50 PDT

Where: Lockpick Vlg

SpeakerBio: Tony Virelli

No BIO available

Description:

Have you ever seen someone just walking around with a key hanging on their belt? How about a wall of keys behind a security desk? Better yet, has anyone you know every posted a picture of the keys to the new home they just bought? Well, what if you could take a picture and easily duplicate that key with a 3D Printer? Sound like something from a James Bond film? Well it's not! Better yet, if you can just get a moment alone with a key, you can get an imprint of it in less than 2 minutes, return the key to the owner and then cast a duplicate of that key for later use.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

Return to Index - Add to  - ics [Calendar](#) file

CRV - Friday - 13:00-13:59 PDT

Title: Key Ingredients for the Job Interviews (Virtual or Face-2-Face)

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Career Hacking VIg

SpeakerBio:Roy Wattanasin

No BIO available

Description:

This presentation focuses on the major key areas to become more successful in your interviews. This includes (6) items: preparation, looking great, resume-review, confidence, note-taking and asking back. This talk will include both considerations when having a virtual or face to face interview(s).

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Friday - 10:10-10:59 PDT

Title: Key Note - State of Blockchain Security

When: Friday, Aug 7, 10:10 - 10:59 PDT

Where: Blockchain VIg

SpeakerBio: Peter Kacherginsky

No BIO available

Description: No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 10:30-10:59 PDT

Title: Keynote Remarks: Representative Jackie Speier

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: Voting Vlg

SpeakerBio: Jackie Speier
Representative Jackie Speier, 14th District, California

Description: No Description available

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar file](#)

VMV - Friday - 14:00-14:30 PDT

Title: Keynote Remarks: Senator Ron Wyden

When: Friday, Aug 7, 14:00 - 14:30 PDT

Where: Voting Vlg

SpeakerBio: Ron Wyden , Senator, Oregon
No BIO available

Description: No Description available

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar file](#)

MOV - Friday - 10:00-11:30 PDT

Title: Keynote: Monero: Sound Money Safe Mode

When: Friday, Aug 7, 10:00 - 11:30 PDT

Where: Monero Vlg

SpeakerBio:Dr. Daniel Kim

No BIO available

Description:

"Monero Means Money" -- with updated data, new data on government budget deficits, and increased emphasis on Monero's importance in the current medical & economic crisis

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Saturday - 10:00-11:30 PDT

Title: Keynote: Monero: Sound Money Safe Mode

When: Saturday, Aug 8, 10:00 - 11:30 PDT

Where: Monero Vlg

SpeakerBio:Dr. Daniel Kim

No BIO available

Description:

"Monero Means Money" -- with updated data, new data on government budget deficits, and increased emphasis on Monero's importance in the current medical & economic crisis

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Sunday - 10:00-11:30 PDT

Title: Keynote: Monero: Sound Money Safe Mode

When: Sunday, Aug 9, 10:00 - 11:30 PDT

Where: Monero Vlg

SpeakerBio:Dr. Daniel Kim

No BIO available

Description:

"Monero Means Money" -- with updated data, new data on government budget deficits, and increased emphasis on Monero's importance in the current medical & economic crisis

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Keynote

When: Friday, Aug 7, 09:00 - 09:59 PDT

Where: ICS Vlg

SpeakerBio:Chris Krebs

Christopher Krebs - serves as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Mr. Krebs was originally sworn in on June 15, 2018 as the Under Secretary for the predecessor of CISA, the National Protection and Programs Directorate (NPPD). Mr. Krebs was nominated for that position by President Trump in February 2018.

Before serving as CISA Director, Mr. Krebs was appointed in August 2017 as the Assistant Secretary for Infrastructure Protection. In the absence of a permanent NPPD Under Secretary at the time, Mr. Krebs took on the role of serving as the Senior Official Performing the Duties of the Under Secretary for NPPD until he was subsequently nominated as the Under Secretary and confirmed by the Senate the following year.

Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

Before Microsoft, Mr. Krebs advised industry and Federal, State, and local government customers on a range of cybersecurity and risk management issues. This is his second tour working at DHS, previously serving as the Senior Advisor to the Assistant Secretary for Infrastructure Protection and playing a formative role in a number of national and international risk management programs.

As Director, Mr. Krebs oversees CISA's efforts to defend civilian networks, manage systemic risk to National critical functions, and work with stakeholders to raise the security baseline of the Nation's cyber and physical infrastructure.

Mr. Krebs holds a bachelor's degree in environmental sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

Description:No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - [ics Calendar file](#)

LPV - Sunday - 13:00-13:30 PDT

Title: Keystone to the Kingdom

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: Lockpick Vlg

SpeakerBio: Austin Marck

No BIO available

Description:

SFICs are very popular locks, but there are some tricks that might get you in the front door. By the end of this talk participants should be familiar with SFIC picking, Key Duplication, Lateral movement, and System decoding. There is even a remote CTF!

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Kibana: An Introduction Into OpenSOC CTF Tools

When: Thursday, Aug 6, 11:15 - 11:59 PDT

Where: Blue Team VIg - Workshop Track 1

SpeakerBio: TimDotZero

No BIO available

Twitter: [@TimDotZero](#)

Description:

Every year the Blue Team Village hosts OpenSOC. A unique defense CTF meant to teach and test practical incident response skills in an environment that's as close to "the real thing" as it gets.

This year BTV wanted to do more. We know that some Blue Teamers might be unfamiliar with some of the tools used by OpenSOC. And we didn't want that to keep anyone from playing this incredible defense simulation.

So this year we are dedicating all day Thursday to demo the various OpenSOC tools, before OpenSOC starts on Friday. These are tools like Graylog, Moloch, Zeek, Osquery, and others that Blue Teamers rely on every day to defend their networks against attackers.

That means that after you LEARN the tools, you can PLAY the OpenSOC CTF, and then take that knowledge back to your own Blue Team to DO the work of defending your network.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOT - Saturday - 12:30-13:15 PDT

Title: Kicking Devices and Taking CVEs : The Zoomer's Guide to Hacking Shit

When: Saturday, Aug 8, 12:30 - 13:15 PDT

Where: IOT VIg

SpeakerBio:Sanjana Sarda

Sanjana Sarda is a Junior Security Analyst at Independent Security Evaluators and is a rising Electrical Engineering senior at UCLA. She is primarily focused on Cryptography, IoT and Hardware Security and hiding from her dog. Sarda has been researching various IoT devices and has discovered several CVEs. Her research has been covered by publications such as Motherboard, the Daily Swig, and ISMG.

Description:

Do you ever play iSpy with the smart devices around you and wonder how easy it is to hack shit and get CVEs? In the Zoomer era, smart devices are extremely accessible, generally cheap and not very security focused. In this talk, Sarda (a fellow Zoomer) will walk the audience through the basic methodology, tooling, exploitation, and disclosure process used when hacking an IoT device. This talk will include a "livish demo of the exploitation of 5 CVEs, including remote code execution and telnet access, discovered while researching the Tenda AC1900 router—which can be chained to provide persistent root shell access to the device

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Killer Robots Reconsidered

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Ethics VIg

Speakers:Diane Vavrichek,Larry Lewis

SpeakerBio:Diane Vavrichek

No BIO available

SpeakerBio:Larry Lewis

No BIO available

Description:

This will be a live talk.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Knock knock, who's there? Identifying assets in the cloud

When: Friday, Aug 7, 08:00 - 08:59 PDT

Where: Red Team VIg

Speakers: Tanner Barnes (aka @_StaticFlow_), NahamSec

SpeakerBio: Tanner Barnes (aka @_StaticFlow_)

Tanner Barnes (aka @StaticFlow) Software engineer and hacker who develops tools for the Cyber Security world. You can find the tools I build on stream here at <https://github.com/Static-Flow>

Twitter: [@_StaticFlow_](#)

SpeakerBio: NahamSec

NahamSec currently works as the Head of Hacked Education at HackerOne by day, and a hacker by night. He has helped identify and exploit over 600 security vulnerabilities across 100+ of web and mobile applications for companies such as Yahoo, Google, Airbnb, Snapchat, The US Department of Defense, Yelp, and more. He also cofounded Bug Bounty Forum, a community of 500+ active hackers sharing ideas and their experiences. He also streams live hacking on Twitch, and create educational content about hacking on YouTube.

Description:

Identifying and enumerating assets has become incredibly easy thanks to all the tools that have been released in the past few years, but being the first to a new target can be the difference between a P1 and a Duplicate! This talk will cover how we were able to monitor, fingerprint, and catalog cloud assets at a rate of over 200 thousand hosts a second in an attempt to find bounty targets and the bugs within them before anyone else.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Kubernetes Container Orchestration Security Assessment

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: AppSec Vlg

SpeakerBio: Ali Abdollahi

Ali Abdollahi is a cyber security expert with over 8 years of experience working in a variety of security fields. Ali is a full-time consultant helping clients with product security testing, reverse engineering, penetration testing, exploit developing, red-teaming, secure coding, and more, giving him ample opportunity to use his skills in a diversity of ways. In addition, He is instructor, author and board of review at Hakin9 company. Ali is a self-confessed bug hunter, publisher of many vulnerabilities and CVEs. Ali is a regular speaker and trainer at industry conferences.

Twitter: [@AliAbdollahi2](#)

Description:

In this workshop, we will first discuss the fundamentals. After grasping underlying containerization technology, we will go deep about technology vulnerabilities, exploitation techniques, auditing, and hardening solutions.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Kubernetes Goat - Vulnerable by Design Kubernetes Cluster Environment

When: Sunday, Aug 9, 09:45 - 10:45 PDT

Where: Red Team Vlg

SpeakerBio:Madhu Akula

Madhu Akula is creator of Kubernetes Goat, security ninja, published author and cloud native security researcher with an extensive experience. Also he is an active member of the international security, devops and cloud native communities (null, DevSecOps, AllDayDevOps, etc). Holds industry certifications like OSCP (Offensive Security Certified Professional), CKA (Certified Kubernetes Administrator), etc. Madhu frequently speaks and runs training sessions at security events and conferences around the world including DEFCON (24, 26 & 27), BlackHat USA (2018 & 19), USENIX LISA (2018 & 19), O'Reilly Velocity EU 2019, GitHub Satellite 2020, Appsec EU (2018 & 19), All Day DevOps (2016, 17, 18, 19 & 20), DevSecCon (London, Singapore, Boston), DevOpsDays India, c0c0n(2017, 18), Nullcon (2018, 19), SACON 2019, Serverless Summit, null and multiple others. His research has identified vulnerabilities in over 200+ companies and organisations including; Google, Microsoft, LinkedIn, eBay, AT&T, WordPress, NTOP and Adobe, etc and credited with multiple CVE's, Acknowledgements and rewards. He is co-author of Security Automation with Ansible2 (ISBN-13: 978-1788394512), which is listed as a technical resource by Red Hat Ansible. Also won 1st prize for building Infrastructure Security Monitoring solution at InMobi flagship hackathon among 100+ engineering teams."

Description:

Kubernetes Goat is "vulnerable by design Kubernetes Cluster environment to practice and learn about Kubernetes Security. In this session Madhu Akula will present how to get started with Kubernetes Goat by exploring different vulnerabilities in Kubernetes Cluster and Containerised environments. Also he demonstrates the real-world vulnerabilities and maps the Kubernetes Goat scenarios with them. Also, we will see the complete documentation and instruction to practice Kubernetes Security for performing security assessments. As a defender you will see how we can learn these attacks, misconfigurations to understand and improve your cloud native infrastructure security posture.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: LadderLeak: Breaking ECDSA With Less Than One Bit Of Nonce Leakage

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Crypto & Privacy Vlg

Speakers: Akira Takahashi, F. Novaes, M. Tibouchi, Y. Yarom, Diego F. Aranha

SpeakerBio: Akira Takahashi

Akira Takahashi is currently a PhD student at Cryptography and Security Group, Aarhus University, Denmark. He was an intern in the Cryptography Research Laboratory at NTT Corporation, Japan and has also worked as a software developer at Richie Oy, Finland. His research interests cover implementation attack on public key cryptographic algorithms and construction of efficient secure two-/multi-party computation protocols. He has given talks about his research projects in different top-tier conferences, including Eurocrypt [3], Euro S&P, and CHES [4].

SpeakerBio: F. Novaes

No BIO available

SpeakerBio: M. Tibouchi

No BIO available

SpeakerBio: Y. Yarom

No BIO available

SpeakerBio: Diego F. Aranha

Diego F. Aranha is an Associate Professor of Computer Science at Aarhus University, Denmark. His professional experience is in Cryptography and Computer Security, with a special interest in the efficient implementation of cryptographic algorithms and security analysis of real-world systems. He received the Google Latin America Research Award for research on privacy twice, and the MIT TechReview's Innovators Under 35 Brazil Award for his work in electronic voting. He has given talks about his research in more than 100 occasions in 10 different countries, including BlackHat Asia [1] and DEF CON Voting Village [2].

Description:

Although it is one of the most popular signature schemes today, ECDSA presents a number of implementation pitfalls, in particular due to the very sensitive nature of the random value (known as the nonce) generated as part of the signing algorithm. It is known that any small amount of nonce exposure or nonce bias can in principle lead to a full key recovery: the key recovery is then a particular instance of Boneh and Venkatesan's hidden number problem (HNP). That observation has been practically exploited in many attacks in the literature, taking advantage of implementation defects or side-channel vulnerabilities in various concrete ECDSA implementations. However, most of the attacks so far have relied on at least 2 bits of nonce bias (except for the special case of curves at the 80-bit security level, for which attacks against 1-bit biases are known, albeit with a very high number of required signatures).

In this paper, we uncover LadderLeak, a novel class of side-channel vulnerabilities in implementations of the Montgomery ladder used in ECDSA scalar multiplication. The vulnerability is in particular present in several recent versions of OpenSSL. However, it leaks less than 1 bit of information about the nonce, in the sense that it reveals the most significant bit of the nonce, but with probability < 1 . Exploiting such a mild leakage would be intractable using techniques present in the literature so far. However, we present a number of theoretical improvements of the Fourier analysis approach to solving the HNP (an approach originally due to Bleichenbacher), and this lets us practically break LadderLeak-vulnerable ECDSA implementations instantiated over the sect163r1 and NIST P-192 elliptic curves. In so doing, we achieve several significant computational records in practical attacks against the HNP.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Lateral Movement and Privilege Escalation in GCP; Compromise any Organization Without Dropping an Implant

When: Sunday, Aug 9, 16:30 - 16:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Allison Donovan, Dylan Ayrey

SpeakerBio: Allison Donovan , Security Engineer

Allison Donovan is a security researcher who specializes in cloud-based platforms and devices. She is currently employed as a Senior Infrastructure Security Engineer at Cruise, where she secures cloud-based environments at scale, and previously she worked at Microsoft on mobile application security and site reliability engineering.

SpeakerBio: Dylan Ayrey , Security Engineer

I'm a Senior Security. I've been heavily involved in the open source community for a few years, and I've been doing my best to bring security practices into the cloud/devsecops world.

Description:

Google Cloud's security model in many ways is quite different from AWS. Spark jobs, Cloud Functions, Jupyter Notebooks, and more default to having administrative capabilities over cloud APIs. Instead of defaulting to no capabilities, permissions are granted to default identities. One default permission these identities have is called actAs, which allows a service by default to assume the identity of every service account in its project; many of which typically have role bindings into other projects and across an organization's resources.

This means by default many API's and identities can compromise large swaths of an organization by moving laterally by impersonating or gaining access to other identities. This can all be done without dropping a single implant on a machine.

In this talk we'll demonstrate several techniques to perform identity compromise via the ActAs permission, privilege escalation, lateral movement, and widespread project compromise in Google Cloud. As well as release tools for exploitation.

Next we'll show what detection capabilities are possible in the Google Cloud ecosystem, by showing Stackdriver logs that correspond with our exploitation techniques, and showing limitations in what's available. We'll also release tools and queries that can be used for detection . As well as insight to how we have attempted to tackle this problem at scale.

Lastly we'll go over remediation efforts you can take as a Google Cloud customer, and show how difficult it can be to secure yourself against these attacks. We will release tools that can be used to harden your organization, and walk through user stories and anecdotes of what this process looks at scale within our organization.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

LPV - Saturday - 13:00-13:45 PDT

Title: Law School for Lockpickers

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: Lockpick Vlg

SpeakerBio: Preston Thomas

No BIO available

Description:

No, Virginia, lockpicks aren't "illegal". Like lockpicking itself, the law of lockpicking is esoteric, widely misunderstood, and occasionally a source of hilarity when interpreted by outsiders. Class is in session as practicing attorney and former TOOOL Board member Preston Thomas hosts a lighthearted law school for locksporters, laying out the legal logic, busting myths, and telling stories. Expect raucous Q&A, real talk, and absolutely zero legal advice.

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Learn to Solder the BadgeBuddy Kit

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Joseph Long (hwbxr)

Joseph Long (hwbxr) is the founder of HackerBoxes: the monthly subscription box for DIY electronics, computer technology, and hacker culture. He has extensive experience in technology R&D and is an attorney of technology law. A former member of the research faculty at Georgia Tech, Joseph is a licensed professional engineer, amateur radio volunteer examiner, past IEEE senior member and chair of multiple IEEE chapters. He has directed or contributed to numerous engineering projects in diverse technology areas including digital and embedded systems, medical devices, broadband communications, and information security. Joseph has provided engineering expertise to technology startups, Fortune 500 companies, NASA, various other government agencies, and research laboratories. He has also prepared and prosecuted hundreds of patent applications for technology leaders such as Google, Microsoft, IBM, AT&T, Cisco, and Boeing as well as technology startups and various university clients.

Description:

Learn to Solder with HackerBoxes. Assemble your very own BadgeBuddy. HackerBoxes has updated a special edition BadgeBuddy soldering kit for DEF CON 28 SAFE MODE.

The BadgeBuddy is a simple and fun kit to introduce basic soldering skills. Once assembled, the blinky mini-badge PCB can be hung from a conference lanyard, backpack, purse, belt, etc using the included bead-chain. The BadgeBuddy uses self-cycling rainbow LEDs for a reduced bill of materials requiring no external control circuitry. The result is a very nice colorful effect that is still simple enough for a first time soldering project.

As in past years, the BadgeBuddy is free (as in beer) and in light of DEF CON 28 SAFE MODE, HackerBoxes will send it directly to you, anywhere in the United States, for only \$1 S&H. If you do not already have soldering tools on hand, HackerBoxes is also making a set of basic soldering tools available at cost. Both can be found at HackerBoxes.com and can be ordered now to ship starting on July 20. Orders as late as July 25 should still be received in time for DEF CON 28 SAFE MODE, but earlier is always better in light of recent postal delays.

#hhv-badgebuddy-qa-text: <https://discord.com/channels/708208267699945503/709254868329693214>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Learn to Solder the BadgeBuddy Kit

When: Saturday, Aug 8, 08:30 - 08:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Joseph Long (hwbxr)

Joseph Long (hwbxr) is the founder of HackerBoxes: the monthly subscription box for DIY electronics, computer technology, and hacker culture. He has extensive experience in technology R&D and is an attorney of technology law. A former member of the research faculty at Georgia Tech, Joseph is a licensed professional engineer, amateur radio volunteer examiner, past IEEE senior member and chair of multiple IEEE chapters. He has directed or contributed to numerous engineering projects in diverse technology areas including digital and embedded systems, medical devices, broadband communications, and information security. Joseph has provided engineering expertise to technology startups, Fortune 500 companies, NASA, various other government agencies, and research laboratories. He has also prepared and prosecuted hundreds of patent applications for technology leaders such as Google, Microsoft, IBM, AT&T, Cisco, and Boeing as well as technology startups and various university clients.

Description:

Learn to Solder with HackerBoxes. Assemble your very own BadgeBuddy. HackerBoxes has updated a special edition BadgeBuddy soldering kit for DEF CON 28 SAFE MODE.

The BadgeBuddy is a simple and fun kit to introduce basic soldering skills. Once assembled, the blinky mini-badge PCB can be hung from a conference lanyard, backpack, purse, belt, etc using the included bead-chain. The BadgeBuddy uses self-cycling rainbow LEDs for a reduced bill of materials requiring no external control circuitry. The result is a very nice colorful effect that is still simple enough for a first time soldering project.

As in past years, the BadgeBuddy is free (as in beer) and in light of DEF CON 28 SAFE MODE, HackerBoxes will send it directly to you, anywhere in the United States, for only \$1 S&H. If you do not already have soldering tools on hand, HackerBoxes is also making a set of basic soldering tools available at cost. Both can be found at HackerBoxes.com and can be ordered now to ship starting on July 20. Orders as late as July 25 should still be received in time for DEF CON 28 SAFE MODE, but earlier is always better in light of recent postal delays.

#hhv-badgebuddy-qa-text: <https://discord.com/channels/708208267699945503/709254868329693214>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Learn to Solder the BadgeBuddy Kit

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Joseph Long (hwbxr)

Joseph Long (hwbxr) is the founder of HackerBoxes: the monthly subscription box for DIY electronics, computer technology, and hacker culture. He has extensive experience in technology R&D and is an attorney of technology law. A former member of the research faculty at Georgia Tech, Joseph is a licensed professional engineer, amateur radio volunteer examiner, past IEEE senior member and chair of multiple IEEE chapters. He has directed or contributed to numerous engineering projects in diverse technology areas including digital and embedded systems, medical devices, broadband communications, and information security. Joseph has provided engineering expertise to technology startups, Fortune 500 companies, NASA, various other government agencies, and research laboratories. He has also prepared and prosecuted hundreds of patent applications for technology leaders such as Google, Microsoft, IBM, AT&T, Cisco, and Boeing as well as technology startups and various university clients.

Description:

Learn to Solder with HackerBoxes. Assemble your very own BadgeBuddy. HackerBoxes has updated a special edition BadgeBuddy soldering kit for DEF CON 28 SAFE MODE.

The BadgeBuddy is a simple and fun kit to introduce basic soldering skills. Once assembled, the blinky mini-badge PCB can be hung from a conference lanyard, backpack, purse, belt, etc using the included bead-chain. The BadgeBuddy uses self-cycling rainbow LEDs for a reduced bill of materials requiring no external control circuitry. The result is a very nice colorful effect that is still simple enough for a first time soldering project.

As in past years, the BadgeBuddy is free (as in beer) and in light of DEF CON 28 SAFE MODE, HackerBoxes will send it directly to you, anywhere in the United States, for only \$1 S&H. If you do not already have soldering tools on hand, HackerBoxes is also making a set of basic soldering tools available at cost. Both can be found at HackerBoxes.com and can be ordered now to ship starting on July 20. Orders as late as July 25 should still be received in time for DEF CON 28 SAFE MODE, but earlier is always better in light of recent postal delays.

#hhv-badgebuddy-qa-text: <https://discord.com/channels/708208267699945503/709254868329693214>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Learn to Solder the BadgeBuddy Kit

When: Sunday, Aug 9, 09:00 - 09:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Joseph Long (hwbxr)

Joseph Long (hwbxr) is the founder of HackerBoxes: the monthly subscription box for DIY electronics, computer technology, and hacker culture. He has extensive experience in technology R&D and is an attorney of technology law. A former member of the research faculty at Georgia Tech, Joseph is a licensed professional engineer, amateur radio volunteer examiner, past IEEE senior member and chair of multiple IEEE chapters. He has directed or contributed to numerous engineering projects in diverse technology areas including digital and embedded systems, medical devices, broadband communications, and information security. Joseph has provided engineering expertise to technology startups, Fortune 500 companies, NASA, various other government agencies, and research laboratories. He has also prepared and prosecuted hundreds of patent applications for technology leaders such as Google, Microsoft, IBM, AT&T, Cisco, and Boeing as well as technology startups and various university clients.

Description:

Learn to Solder with HackerBoxes. Assemble your very own BadgeBuddy. HackerBoxes has updated a special edition BadgeBuddy soldering kit for DEF CON 28 SAFE MODE.

The BadgeBuddy is a simple and fun kit to introduce basic soldering skills. Once assembled, the blinky mini-badge PCB can be hung from a conference lanyard, backpack, purse, belt, etc using the included bead-chain. The BadgeBuddy uses self-cycling rainbow LEDs for a reduced bill of materials requiring no external control circuitry. The result is a very nice colorful effect that is still simple enough for a first time soldering project.

As in past years, the BadgeBuddy is free (as in beer) and in light of DEF CON 28 SAFE MODE, HackerBoxes will send it directly to you, anywhere in the United States, for only \$1 S&H. If you do not already have soldering tools on hand, HackerBoxes is also making a set of basic soldering tools available at cost. Both can be found at HackerBoxes.com and can be ordered now to ship starting on July 20. Orders as late as July 25 should still be received in time for DEF CON 28 SAFE MODE, but earlier is always better in light of recent postal delays.

#hhv-badgebuddy-qa-text: <https://discord.com/channels/708208267699945503/709254868329693214>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Learn to Solder the BadgeBuddy Kit

When: Sunday, Aug 9, 14:00 - 14:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Joseph Long (hwbxr)

Joseph Long (hwbxr) is the founder of HackerBoxes: the monthly subscription box for DIY electronics, computer technology, and hacker culture. He has extensive experience in technology R&D and is an attorney of technology law. A former member of the research faculty at Georgia Tech, Joseph is a licensed professional engineer, amateur radio volunteer examiner, past IEEE senior member and chair of multiple IEEE chapters. He has directed or contributed to numerous engineering projects in diverse technology areas including digital and embedded systems, medical devices, broadband communications, and information security. Joseph has provided engineering expertise to technology startups, Fortune 500 companies, NASA, various other government agencies, and research laboratories. He has also prepared and prosecuted hundreds of patent applications for technology leaders such as Google, Microsoft, IBM, AT&T, Cisco, and Boeing as well as technology startups and various university clients.

Description:

Learn to Solder with HackerBoxes. Assemble your very own BadgeBuddy. HackerBoxes has updated a special edition BadgeBuddy soldering kit for DEF CON 28 SAFE MODE.

The BadgeBuddy is a simple and fun kit to introduce basic soldering skills. Once assembled, the blinky mini-badge PCB can be hung from a conference lanyard, backpack, purse, belt, etc using the included bead-chain. The BadgeBuddy uses self-cycling rainbow LEDs for a reduced bill of materials requiring no external control circuitry. The result is a very nice colorful effect that is still simple enough for a first time soldering project.

As in past years, the BadgeBuddy is free (as in beer) and in light of DEF CON 28 SAFE MODE, HackerBoxes will send it directly to you, anywhere in the United States, for only \$1 S&H. If you do not already have soldering tools on hand, HackerBoxes is also making a set of basic soldering tools available at cost. Both can be found at HackerBoxes.com and can be ordered now to ship starting on July 20. Orders as late as July 25 should still be received in time for DEF CON 28 SAFE MODE, but earlier is always better in light of recent postal delays.

#hhv-badgebuddy-qa-text: <https://discord.com/channels/708208267699945503/709254868329693214>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOT - Saturday - 15:30-16:30 PDT

Title: Learning to Use Logic Analyzers

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: IOT VIg

SpeakerBio:Jonathan Stines

Jonathan is a Senior Security Consultant on Rapid7's Penetration Testing team and has 7 years of pen test and consulting experience. Jonathan has worked on a wide breadth of projects, ranging from hacking a regional bank's LAN network in Wales to breaking into a Chinese warehouse's wireless network in Guangdong. With a specialization in hacking IoT and embedded systems, Jonathan has a tendency of raiding local garage sales and thrift stores in search of the next gadget to tear into.

Description:

This learning session attendees will learn how to properly utilize a logic analyzer for examining, testing and decoding digital communication on embedded systems. Also, various logic analyzers from cheap models to the more expensive models will be shown and discussed. After each learning objective we will have Q&A sessions.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Least privilege using infrastructure as code

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: Cloud Vlg

SpeakerBio: Nimrod Kor

Nimrod cloud security engineers team lead. He is an open source contributor to various AWS security projects and also part of Bridgecrew's founding team. A believer in terraform as a security enabler.

Description:

Security teams in the cloud are faced with an overwhelming amount of information to process in order to keep their environments secure. Keeping up with everything manually is a difficult, never-ending task where failure can have high consequences. Permissions management can be a time-consuming task, and as a security engineer, you'd often ask your self "how should have access to what? ", "who have access it in the past? and "Is it OK to remediate those excessive permissions or would it cause a downtime?".

In this talk, we will demonstrate a method to automatically secure a live AWS IAM environment to a specific, less-permissive role that best fits the access pattern using the open-source tool: <https://github.com/bridgecrewio/AirIAM/> . At the end of the talk, we will have a result in Terraform code with a much smaller attack surface and reduced risk.

YouTube: https://www.youtube.com/watch?v=gwBG_oKDINQ

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Length 15 & No Change. Implementing NIST SP800-63B for real (Rebroadcast)

When: Saturday, Aug 8, 22:00 - 22:59 PDT

Where: Password Vlg

SpeakerBio:Per Thorsheim

Per Thorsheim is the founder of PasswordsCon. By day he works as CSO of a large hotel chain in northern europe, holds multiple relevant certifications & bla bla bla. By evening, night, weekends & vacations he is passionate about passwords, digital authentication, email & DNS security/privacy.

He has spoken at conferences in many countries around the world (including Cryptovillage!), and is frequently interviewed in media. He is known for his passionate & easy to understand presentations, mixing technical topics with humor, stories from real life & practical advice.

Description:No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Leveraging the critical YARA skills for Blue Teamers (Beginner)

When: Saturday, Aug 8, 09:00 - 10:30 PDT

Where: Blue Team Vlg - Workshop Track 1

SpeakerBio:David Bernal Michelena

David Bernal Michelena holds a bachelor's degree in Computer Engineering from the National Autonomous University of Mexico (UNAM) and 10 industry security certifications. He is a Senior Incident Handler Consultant in Mandiant and formerly has worked as Lead Security Researcher, Forensic Analyst and Digital Handler in both private and educational security organizations. David has spoken in various security conferences, such as Black Hat USA, SANS Threat Hunting Summit, Digital Crimes Consortium, 8.8 and BSidesCDMX. On his free time, he likes to code, swim and play music.

Twitter: [@d4v3c0d3r](#)

Description:

YARA rules have become one of the de facto industry standards for threat detection on files. It is important that blue teamers know what are YARA rules and the basic skills to correctly leverage them on file system, memory dumps and traffic analysis. This is useful for multiple blue team roles mainly malware researchers, security analysts, threat hunters and intelligence analyst.

YARA rules have become one of the de facto industry standards for threat detection on files. It is important that blue teamers know what are YARA rules and the basic skills to correctly leverage them on file system, memory dumps and traffic analysis. This is useful for multiple blue team roles mainly malware researchers, security analysts, threat hunters and intelligence analyst.

Writing YARA rules

Reading YARA rules

Enhancing YARA rules

I will prepare a LINUX virtual machine that will be given to the attendees with some malware samples, memory dumps and pcaps and they will perform various exercises to learn the basic YARA skills. In this training, the attendees will learn:

- How to install on Linux and Windows
- How to develop several YARA rules for several malware samples
- How to do targeted scans with YARA on file system
- How to do memory YARA scans with volatility and recall
- How to YARA scan files on the network traffic
- Video showing YARA detection on malicious files on pcap
- Tool for automatically extracting and analyzing files with YARA rules on network traffic created by the author (YARAZeek)
- Getting open YARA open source rules from well-known security researchers and other reputable sources.
- Using VirusTotal Retrohunt

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 20:00-20:59 PDT

Title: Live Q&A with Special Guests Regarding "Kill Chain"

When: Friday, Aug 7, 20:00 - 20:59 PDT

Where: Voting Vlg

Description:

Exciting News for DEF CON Safe Mode! Voting Village and HBO have arranged for a limited time FREE access to the Kill Chain Documentary on YouTube!

In conjunction, the Voting Village will host a LIVE Q + A with SPECIAL GUESTS at 20:00 on FRIDAY August 7.

View the Q and A on the Voting Village Twitch and YouTube streams; there is ongoing discussion on Discord in #vmhv-talks-text, and you can submit questions at #vmhv-talks-questions-text.

Movie: <https://www.youtube.com/watch?v=nQuwTdrVrg4>

Village YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Village Twitch: <https://www.twitch.tv/votingvillagedc/about>

Store: <https://www.bonfire.com/store/eif/>

#vmhv-talks-text: <https://discord.com/channels/708208267699945503/737818386796511312>

#vmhv-talks-questions-text: <https://discord.com/channels/708208267699945503/737818504627093575>

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

SEV - Friday - 13:00-13:59 PDT

Title: Live SE Q&A

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Social Engineer Village

Description:

#sev-qa-voice: <https://discord.com/channels/708208267699945503/736686395631992852>

Return to Index - Add to  - ics [Calendar](#) file

Title: lo57 Mystery Challenge

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231985>

Discord: <https://discord.com/channels/708208267699945503/732439421973954571>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: lo57 Mystery Challenge

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231985>

Discord: <https://discord.com/channels/708208267699945503/732439421973954571>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: lo57 Mystery Challenge

When: Sunday, Aug 9, 00:00 - 15:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231985>

Discord: <https://discord.com/channels/708208267699945503/732439421973954571>

[Return to Index](#) - Add to  - ics [Calendar file](#)

ASV - Saturday - 13:00-13:45 PDT

Title: localhost: Escaping the Browser Sandbox Without 0-Days

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: AppSec Vlg

SpeakerBio: Parsia Hakimian

No BIO available

Twitter: [@cryptogangsta](#)

Description: No Description available

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Sunday - 13:00-13:30 PDT

Title: Locha Mesh: Monero off-the-grid

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: Monero Vlg

SpeakerBio:Randy Brito

No BIO available

Description:No Description available

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Low Value Indicators For High Value Decisions (Intermediate)

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: Blue Team Vlg - Talks Track 1

Speakers: Allan Stojanovic, Spencer Cureton

SpeakerBio: Allan Stojanovic

Allan Stojanovic has survived IT for over 25 years. He has worked in nearly every vertical doing many different roles, mostly in the Information Security field. A jack of all trades, Allan tries to know a little bit about everything, and is a self-proclaimed expert at nothing.

Twitter: [@allansto](#)

SpeakerBio: Spencer Cureton

No BIO available

Description:

We will present how the Abuse Operations team uses collections of indicators to fingerprint and track adversaries on one of the largest pure-play, remote-code-execution-as-a-service platforms on the Internet: Heroku. We can detect when they change tactics, we can spot the number of people involved, and we can misdirect them to the point that they become even easier to track!

We hope the ideas presented here will help your day to day routine as well as provide a solid model to guide future decisions from architecture to automation.

Introduction

Allan and Spencer

Heroku - A PaaS that's basically RCEaaS We keep customers from doing bad things on, to, and from the platform

Adversaries

Adversary classification and evolution - skids to apex threat actors Establishing intent to differentiate good from bad actor.

Definitions

"Abuse" - misuse, malice, crime

Indicators, TTPs, Fingerprints

Slang: splash, pivot, etc.

Methodology

Hunting - environment and tools (and lack of) Leveraging the home field advantage Determining intent with constellation of indicators Detecting adversary changes when pressure is applied - from TTP shifts to spotting multiple actors from a campaign Leading the adversary - limit their available choices

Examples of frustrating specific actors/campaigns

Cryptocurrency mining

Phishing

Blackhat SEO

Takeaways

Break spirits, not code!

Identify all sources of indicators - internal and external TI All low value indicators are equal until they are not.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Low-Cost VHF Receiver: Eavesdropping Pilot/Controller Communication

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Aerospace VIg

Speakers: Allan Tart, Fabian Landis

SpeakerBio: Allan Tart

Allan Tart joined OpenSky network in July 2019, where his main responsibilities include leading special research and development projects. He has more than a decade worth of experience working in the air traffic management domain, where he has filled different positions ranging from being surveillance systems engineer to leading various development projects. In addition to his work in ATM, he has been actively conducting research in the field of array processing and spatial filtering at Tallinn University of Technology. In recent years his research interests have shifted toward the area of radio network deployment, in which he cooperates with the Standards and Technology department in Ericsson AB.

SpeakerBio: Fabian Landis

Fabian Landis received his master's degree at the Swiss Federal Institute of Technology Zurich in 2004 in the areas of computer networks, computer vision, IT security and speech processing. He has been a developer since, working for banks and software providers in the area of infrastructure, trade finance and IAM. He has recently joined Opensky Networks and is now focusing on the ATCO2 project which this talk will cover to some extent.

Description:

The objective of the talk is to give an overview of the latest development in OpenSky Network – recording Air Traffic Control ATC voice communications.

As the receiver-feeder system will be developed within ATCO2 project, an undertaking financed by the European Union, a short overview of the ATCO2 project will be given. The central question covered in this first part of the talk is: “What will happen with the voice recording after it’s uploaded to OpenSky Network?”

The main part of the talk will focus on how to set up the receiver which is built around RTLSDR-Airband - an open source multichannel AM/NFM receiver (more about it here: <https://github.com/szpajder/RTLSDR-Airband/wiki>).

Participants are encouraged to take an active role during the workshop and set up the receiver during the talk. In order to do that, listeners should make sure they have the following items available: - Raspberry Pi (any version should work). - SDR-RTL dongle (RTL-SDR Blog R820T2 RTL2832U 1PPM TCXO SMA Software Defined Radio with Dipole Antenna Kit available from <https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/> as includes antenna and antenna cables). - SD card (with memory of 16GB is sufficient)

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

Github: <https://github.com/szpajder/RTLSDR-Airband/wiki>

Return to Index - Add to  - ics [Calendar](#) file

Title: Making Breach and Attack Simulation Accessible and Actionable with Infection Monkey - from IT to the C-suite

When: Thursday, Aug 6, 20:30 - 21:30 PDT

Where: Red Team VIg

SpeakerBio: Shay Nehmad

Shay Nehmad is a lead developer at Guardicore, where he is working on the Infection Monkey, an open-source breach and attack simulation tool. Over the last few years in the IDF, Shay amassed extensive experience in both Information Security and Software Development.

Description:

Oftentimes one of the greatest challenges for security professionals today is finding a way to effectively communicate the state of a network's security posture, and what steps are necessary to achieve the organization's security goals. Red teamers are already familiar with executing a typical Breach and Attack simulation, but how can they take greater advantage of their findings, and better yet, share those with the C-suite? The Infection Monkey is a mature, widely-used Open Source GPLv3 licensed tool specifically developed for enterprise red teams. Designed to test an organization's detection and response methods and teams, the Monkey simulates all steps of an attack by mimicking a variety of adversary moves such as scanning, exploitation, lateral movement, password stealing, network mapping, security control bypass and more. Overall, the Infection Monkey's simulation reveals it contains a lot of stages one might find in a manual penetration test (or in a real attack). The Monkey is easily configurable, and starts from a single machine and propagates according to the test scenario while collecting data, employing attack tactics, performing security tests and looking for more machines to attack. The results are generated in real-time, shown in a network map and also presented in 3 detailed reports. With the Monkey, red teams can autonomously test specific parts of the network with multiple attack scenarios on a regular basis - like executing a lateral movement scenario from an internet-facing server to a sensitive system deployed in a different part of the network. Further, the Monkey maps its findings to both the MITRE ATT&CK knowledgebase and Forrester's Zero Trust framework to provide in-depth reports with actionable recommendations for achieving a stronger security posture. When mapping to the Zero Trust framework, the report identifies and prioritizes the steps and decisions required to achieve a true Zero Trust network - whether that's verifying that the current security stack meets Zero trust requirements or outlining specific actions that blue teams can perform to implement better security measures. By mapping the reports to MITRE ATT&CK, the Monkey communicates the results of the attack in plain language, making the advanced tool accessible and effective for any red team. These reports enable security professionals to address and improve their security posture using the metrics, methods, and ideas they already care about aka if your CISO wants to achieve Zero Trust, their team can clearly map out the steps required to get there with the Monkey's reports. In this talk, Penetration Testers, Network Engineers, Exploit Developers, and other Security professionals will experience a typical Breach & Attack simulation through the lens of the Monkey to learn how open source solutions can improve and add efficiencies to their teams. Shay will take attendees through a demo of Infection Monkey to demonstrate a typical "before and after" scenario with the Monkey. He will run the Monkey in a test environment, aka the "before," to identify security gaps and then mitigate the issues using advice offered by the Monkey's reporting. Finally, Shay will run the Monkey in the "after" environment to show how effective this Breach and Attack simulation can be in strengthening security posture.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar file](#)

Title: Making Next Generation Drugs at Home

When: Sunday, Aug 9, 13:30 - 14:30 PDT

Where: BioHacking Vlg

SpeakerBio:Mixæl Swan Laufer

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. Perpetually disruptive, he continues to work to make it possible for people to manufacture their own medications at home.

Description:

The structures of drugs and their delivery mechanisms have become orders of magnitude more sophisticated in recent years. Polymer subdermal trickle-delivery implants can now be manufactured with a 3D printer filament extruder. We can now find simple new synthesis pathways for complex molecules using machine learning systems, and these compounds can be made at home. The Four Thieves Vinegar Collective will show the free, open access, supercomputing platform they have built so that anyone can do research in this arena independently on our hardware. Additionally, they will show the latest version of the automated chemical reactor, the Apothecary Microlab, which requires no soldering, and is built entirely from off-the-shelf and 3D printed parts.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Making sense of EMV card data – decoding the TLV format

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Payment Vlg

SpeakerBio: Dr Steven J. Murdoch

No BIO available

Description:

EMV (sometimes known as Chip and PIN) is the worldwide standard for smart card payments. It was designed to allow credit and debit cards issued by any bank work to make a payment through any terminal, even across international borders and despite chip cards being extremely limited in the computation they can perform. In this talk I'll discuss how EMV achieves this difficult task, through the use of the TLV (Tag-Length-Value) data format. I will demonstrate how to decode TLV data found on real EMV chip cards, and what significance this data has in the wider payment ecosystem. Finally I'll discuss how the use of TLV, despite its advantages, has contributed to the creation of security vulnerabilities in Chip and PIN.

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 21:30-21:59 PDT

Title: Making Targeted Wordlists (Rebroadcast)

When: Friday, Aug 7, 21:30 - 21:59 PDT

Where: Password Vlg

SpeakerBio: Password Village Staff
No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 13:00-13:30 PDT

Title: Making Targeted Wordlists

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: Password Vlg

SpeakerBio: Password Village Staff
No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: MalConfScan with Cuckoo

When: Sunday, Aug 9, 10:00 - 11:50 PDT

Where: See Description or Village

Speakers: Tomoaki Tani, Shusei Tomonaga

SpeakerBio: Tomoaki Tani

Tomoaki Tani works as a Forensic Analyst at Incident Response Group of JPCERT/CC. His primary responsibility is in providing coordination and assistance for cybersecurity incidents related to Japanese constituents. With his technical insight, he is also in charge of analyzing incident trends and attack methods. He presented at CODE BLUE, BsidesLV, BlackHat USA Arsenal, PHDays, VB Conference, and more. Prior to joining JPCERT/CC, he was engaged in security analysis operations and incident handling at a major Japanese telco.

SpeakerBio: Shusei Tomonaga

Shusei Tomonaga is a member of the Incident Response Group of JPCERT/CC. Since December 2012, he has been engaged in malware analysis and forensic investigation. In particular, he spearheads the analysis of targeted attacks affecting critical Japanese industries. In addition, he has written blog posts on malware analysis and technical findings (<https://blogs.jpCERT.or.jp/en/>). Prior to joining JPCERT/CC, he was engaged in security monitoring and analysis operations at a foreign-affiliated IT vendor. He has presented at CODE BLUE, BsidesLV, Botconf, VB Conference, PHDays, PacSec, FIRST Conference, BlackHat USA Arsenal, and more.

Description:

"MalConfScan with Cuckoo" is a tool for automatically extracting known Windows and Linux malware's configuration data.

Audience: Defense (Malware Analyst, BlueTeam)

Interact @ #dl-tani-malconfscan-text: <https://discord.com/channels/708208267699945503/730256507702345813>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://github.com/JPCERTCC/MalConfScan-with-Cuckoo>

Forum: <https://forum.defcon.org/node/233121>

Return to Index - Add to  - ics [Calendar](#) file

Title: Mechanizing the Methodology: Automating Discovery, Testing, and Alerting using Recon/Testing Tools and Amazon SES

When: Saturday, Aug 8, 08:30 - 09:30 PDT

Where: Red Team Vlg

SpeakerBio: Daniel Miessler

Daniel Miessler is a recognized cybersecurity expert and writer with 20 years in Information Security. His experience ranges from technical assessment and implementation, to executive level advisory services consulting, to building and running industry-leading security programs. His 20 years of experience in security ranges from the vibrant startup ecosystem in his birthplace of Silicon Valley, to working with many of the top 100 worldwide companies. He frequently gives talks and participates in panels around the world, and his work and commentary have been featured in dozens of the world's leading publications.

Description:

There are a million techniques out there for finding new attack surface and finding potential vulnerabilities; the problem is finding the time to run your entire methodology against all your targets. This talk will take you through finding new attack surface, performing multiple types of test against those targets, and sending real-time alerts---all on a continuous basis using automation from a cloud-based Linux host.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Media Analysis of Disinformation Campaigns

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Packet Hacking VIg - Talk

Speakers: Chet Hosmer, Mike Raggio

SpeakerBio: Chet Hosmer , Owner, Python Forensics

Chet Hosmer (Twitter: @chethosmer) is an international author, educator & researcher, and founder of Python Forensics, Inc., a non-profit research institute focused on the collaborative development of open source investigative technologies using the Python programming language. Chet is also a Visiting Professor at Utica College in the Cybersecurity Graduate Program, where his research and teaching is focused on data hiding, active cyber defense and security of industrial control systems. Additionally, Chet is an Adjunct Professor at Champlain College in the Digital Forensics Graduate Program, where his research and teaching is focused on solving hard digital investigation problems using the Python programming language. Twitter: @chethosmer

SpeakerBio: Mike Raggio , Co-Founder, SilentSignals.com

Mike Raggio (Twitter: @MikeRaggio) has over 20 years of security research experience. Over the years he has uncovered numerous vulnerabilities in commercial networking, mobile, and security products. His current research focuses on multimedia disinformation campaigns. His research has been highlighted on television's CNN Tech, and numerous media publications including TIME, Forbes, Bloomberg, Dark Reading, TechCrunch, TechTarget, The Register, and countless others. Michael is the author of "Mobile Data Loss: Threats & Countermeasures" and "Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols" for Syngress Books, and is a contributing author for "Information Security the Complete Reference 2nd Edition". His Data Hiding book is also included at the NSA's National Cryptologic Museum at Ft. Meade. A former security trainer, Michael has briefed international defense agencies including the FBI, Pentagon, and Queensland Police; and is a former participating member of FSISAC/BITS and the PCI Council. He is also a frequent presenter at security conferences, including Black Hat, DEF CON, Gartner, RSA, DoD Cyber Crime, OWASP, HackCon Norway, and SANS. He was also awarded the Pentagon's Certificate of Appreciation.

Twitter: @MikeRaggio

Description:

In this session we'll focus on the media aspects of disinformation campaigns with deep analysis of altered images, audio, and video to uncover methods used to twist narratives and mislead perceptions surrounding topical news stories. We'll dive into the taxonomy of fake photos, deepfakes, phishing audio fraud attacks, keyword squatting malware, fake rallies, narrative laundering, nation state fake intelligence. and media generated to inspire mass hysteria. We'll then further categorize these threats by their TTPs and provide methods for enhancing detection and response strategies. Real world examples will be demonstrated to provide deep and tangible insights into this systemic problem.

YouTube: <http://youtube.com/wallofsheep>

Twitch: <http://twitch.tv/wallofsheep>

Facebook: <http://facebook.com/wallofsheep/>

Periscope: <https://t.co/gn17JLlftA?amp=1>

Return to Index - Add to  - ics [Calendar](#) file

Title: Medical Device Vulnerability Disclosure

When: Friday, Aug 7, 14:30 - 15:30 PDT

Where: BioHacking Vlg

Speakers:Chloé Messdaghi,Eirick Lurass,Casey John Ellis

SpeakerBio:Chloé Messdaghi

Chloé Messdaghi is the VP of Strategy at Point3 Security. She is a security researcher advocate who strongly believes that information security is a humanitarian issue. Besides her passion to keep people safe and empowered online & offline, she is driven to fight for hacker rights. She is the founder of WomenHackerz & the President and cofounder of Women of Security (WoSEC), podcaster for ITSP Magazine's The Uncommon Journey, and runs the Hacker Book Club.

SpeakerBio:Eirick Lurass

Eirick Lurass is a Chaotic Good Dual-class warrior mage. After trying many jobs, he eventually found out he could do magical things with computers. He works in MedSec and he spends most of his time failing and hearing no. His cats and dog still love him.

SpeakerBio:Casey John Ellis , Founder and CTO, Bugcrowd

Casey Ellis is the Founder, Chairman and CTO of Bugcrowd and the co-founder of the The disclose.io Project. Casey has been making computers, companies, and markets misbehave for great justice since his youth, and pioneered the crowdsourced security-as-a-service industry in 2012.

Description:

Humans write code, humans make mistakes, and hackers are here to help. While this has been true since the beginning of the Internet, 2020 still see's laws like the DMCA and CFAA create a chilling effect on establishing a healthy "Internet immune system" between builders and breakers. In safety critical technology domains like Medical and Medical Devices, this has become especially obvious, and particularly urgent to solve. This mini-panel will run through the past, current, and future state of vulnerability disclosure in the medical sector; provide examples of where it has been needed, gone well, and where it has failed; and ends with an introduction to the The disclose.io Project and some practical steps that anyone in the audience can take to improve the ubiquity of healthy hacker/vendor relationships.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Medical Technology: How do we unfuck things

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: BioHacking Vlg

SpeakerBio: Veronica

Veronica started her forensic career in 2008. She is the Director of Incident Response within DFIRLABS. Veronica is also an Assistant Professor at Noroff University, where she will be given her own Minions to plan her world domination. Veronica holds a Master in Science at Rhodes University in Information Security with specialisation in the forensic analysis of malware. She prides herself in keeping patients safe as this is something which is near to her heart. She is also a cyborg sporting an embedded medical device herself. She also is a DEF CON Goon and she is the founder of DC2751. Her particular research interests include research into security vulnerabilities in medical devices forming part of the Internet of Things, and how these could be exploited by malicious attackers, as well as what types of forensic artefacts could be identified from any attacks. She is extremely passionate about protecting people whose lives depend on these medical devices, and her passion saw her becoming a researcher within an MDM . At her core Veronica is a forensicator and hacker and in love with every bit, byte and nibble of knowledge she has obtained.

Description:No Description available

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: MedICS

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: BioHacking Vlg

SpeakerBio: Bryson Bort

Founder of SCYTHE, next generation attack emulation platform; GRIMM, cybersecurity consultancy; ICS Village Co-Founder, 501c3 for ICS security awareness. Senior Fellow for Cyber/National Security at R Street and National Security Institute; Advisor to the Army Cyber Institute and DHS/CISA.

Description:

Cover what is ICS (industrial control systems), system architecture and typical hospital deployments, threat actors, and security roles and responsibilities (government, user, manufacturers).

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - [ics Calendar file](#)

HHV - Friday - 18:00-18:59 PDT

Title: Meetup: 3H: Hardware Happy Hour

When: Friday, Aug 7, 18:00 - 18:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio:Chris Gammell

No BIO available

Description:

Wind down the first official day of DEF CON Safe Mode talking about hardware! Bring a project to share! All hardware projects are welcome, from a simple Arduino based thingamabob to your company's newest hardware product (and how you earn your living). The main focus is meeting like minded people who are building fun things!

#hhv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 16:00-16:30 PDT

Title: Meetup: Certification Processes (UL, FCC, etc.)

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: ShortTie

No BIO available

Description:

A place to meet people with the same interests or challenges and discuss. The meetup is a nexus for finding and starting the conversation. Bring your expertise and your questions.

#hhv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 15:30-15:59 PDT

Title: Meetup: Legacy Hardware

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio: ShortTie

No BIO available

Description:

A place to meet people with the same interests or challenges and discuss. The meetup is a nexus for finding and starting the conversation. Bring your expertise and your questions.

#hhv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 15:00-15:30 PDT

Title: Meetup: OSS ASIC

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: Josh Marks

No BIO available

Description:

Come geek out about the new Google + efabless + Skywater 130 nm Process Design Kit that was recently released. Brainstorm IC design ideas for the free fab runs in November and in 2021 — an extraordinary value!! No ASIC knowledge? No problem — casual conversation about transistor structures, and basic circuit architectures included.

#hhv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 14:30-14:59 PDT

Title: Meetup: PCB Proto and Rework

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio: ShortTie

No BIO available

Description:

A place to meet people with the same interests or challenges and discuss. The meetup is a nexus for finding and starting the conversation. Bring your expertise and your questions.

#hvv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hvv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 09:30-09:59 PDT

Title: Meetup: Some HHV Challenges

When: Friday, Aug 7, 09:30 - 09:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio:rehr

No BIO available

Description:

HHV members have created a few challenges for this year's DEF CON. Come learn and chat about those challenges, or bring new challenges to share with the community. This time will start with an introduction to this year's HHV challenges, but the remaining time will be open to community questions and conversations.

#hhv-challenge-text: <https://discord.com/channels/708208267699945503/739567199647301702>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Friday - 17:30-17:59 PDT

Title: Meetup: Some HHV Challenges

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio:rehr

No BIO available

Description:

HHV members have created a few challenges for this year's DEF CON. Come learn and chat about those challenges, or bring new challenges to share with the community. This time will start with an introduction to this year's HHV challenges, but the remaining time will be open to community questions and conversations

#hhv-challenge-text: <https://discord.com/channels/708208267699945503/739567199647301702>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 13:00-13:30 PDT

Title: Meetup: Some HHV Challenges

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio:rehr

No BIO available

Description:

HHV members have created a few challenges for this year's DEF CON. Come learn and chat about those challenges, or bring new challenges to share with the community. This time will start with an introduction to this year's HHV challenges, but the remaining time will be open to community questions and conversations.

#hvv-challenge-text: <https://discord.com/channels/708208267699945503/739567199647301702>

#hvv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Saturday - 14:00-14:30 PDT

Title: Meetup: Sourcing Parts

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: bombnav

No BIO available

Description:

Sourcing parts in the COVID involves new challenges due to supply chain issues. Counterfeiting continues to be a problem with out of production parts. This meetup is designed to share ideas and sources for acquiring parts for electronic hobbyists.

#hhv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Sunday - 10:00-10:30 PDT

Title: Meetup: Sourcing Parts

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: Hardware Hacking Vlg

SpeakerBio: bombnav

No BIO available

Description:

Sourcing parts in the COVID involves new challenges due to supply chain issues. Counterfeiting continues to be a problem with out of production parts. This meetup is designed to share ideas and sources for acquiring parts for electronic hobbyists.

#hhv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hhv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HHV - Sunday - 12:30-12:59 PDT

Title: Meetup: Wearables

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: Hardware Hacking Vlg

SpeakerBio: ShortTie

No BIO available

Description:

A place to meet people with the same interests or challenges and discuss. The meetup is a nexus for finding and starting the conversation. Bring your expertise and your questions.

#hvv-meetups-a-text: <https://discord.com/channels/708208267699945503/739567085004521533>

#hvv-meetups-a-voice: <https://discord.com/channels/708208267699945503/739571117756383333>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Mica Husky

When: Saturday, Aug 8, 19:00 - 19:59 PDT

Where: See Description or Village

Description:

Mica has been absolutely obsessed with electronic music since she was a small child. She has been producing electronica for over a decade and DJing at house parties and conventions for 5 years. She first discovered psytrance in particular after going to Equinox 2015 because it "sounded fun". She was instantly hooked. Mica's favorite noises are reminiscent of psychedelic crystals shattering into a million pieces on a forest floor. She can take a crowd on a journey through the world of psychedelia by catching them at the perfect time with the best of alien music.

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Web: <http://www.barkbarkbarkbark.com>

Return to Index - Add to  - ics [Calendar](#) file

POV - Saturday - 16:00-16:59 PDT

Title: Mis/Dis Information & Democracy

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: See Description or Village

Description:

This event requires registration. Please see the below link for more information.

Registration:

<https://www.eventbrite.com/e/def-con-policy-community-roundtable-misdis-information-democracy-tickets-115984678295>

Return to Index - Add to  - ics [Calendar file](#)

Title: Misbehavior Detection for V2X communication

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: Car Hacking Vlg 001

SpeakerBio:Jaime

Jaime is an EE turned software developer turned security researcher. She caught the infosec bug through playing CTFs, and now works at GRIMM hacking cars. In her spare time, she adds LEDs to things and hangs out with her dog.

Description:

In this talk, we will present network attacks that aim at fooling V2X applications. Then, we will show how our misbehavior detection system can detect such attacks. We will also demonstrate the progression of an attacker that becomes smarter and smarter in order to highlight the limitations of current misbehavior detection systems. Attacks and defenses will be shown working on production-ready onboard unit.

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUejlQ&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Saturday - 10:00-10:30 PDT

Title: Misinformation & Covid

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: AI Vlg

SpeakerBio:lmeyerov

No BIO available

Twitter: [@lmeyerov](https://twitter.com/lmeyerov)

Description:No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Miss Jackalope

When: Saturday, Aug 8, 22:00 - 22:59 PDT

Where: See Description or Village

Description:

DEF CON's Resident Community DJ. Miss Jackalope has been DJing drum and bass and breakbeats for a long time and doing InfoSec stuff, too! (\$dayjob) She can be seen DJing parties, swagulating in the Vendor room, and making sure everyone is having a good time. Mega thanks to the Jackalope Army for their support.

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Twitter: <https://twitter.com/djjackalope>

Web: <https://missjackalope.com>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Mission Alenium: Launching the Next Generation into an Immersive Cybersecurity and Space Systems Challenge

When: Friday, Aug 7, 09:00 - 15:59 PDT

Where: Aerospace Vlg

SpeakerBio: Henry Danielson

No BIO available

Description:

The Convergence of Space and Cybersecurity is here! The goal of this immersive, two-part challenge is to expose beginner-level participants to Space Networks, Cybersecurity, Satellites, IoT devices and Digital Forensics Analysis through a gamified satellite cybercrime scenario. The first part includes a series of five online 3D “escape rooms” which each simulate different locations that contain important evidence. After all the information is collected, participants enter the second phase of the challenge and begin conducting forensic analysis. Participants will respond to a fictional storyline where the flight control system of a Low Earth Orbit (LEO) is compromised. Due to the hack, the rocket and its accompanying satellite crash before reaching orbit. The software payload survives the crash and is sufficiently intact for digital forensic analysis. The participants act as cybersecurity digital forensics analysts, attempting to find out how and why the system was hacked and by whom. It is being deployed at the California Cyber Innovation Challenge 2020, the state championship for cybersecurity competitions in California, for teams of middle school and high school students this upcoming October.

Discord: <https://discord.com/channels/708208267699945503/732393009215176854>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Mission Alenium: Launching the Next Generation into an Immersive Cybersecurity and Space Systems Challenge

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: Aerospace Vlg

SpeakerBio: Henry Danielson

No BIO available

Description:

The Convergence of Space and Cybersecurity is here! The goal of this immersive, two-part challenge is to expose beginner-level participants to Space Networks, Cybersecurity, Satellites, IoT devices and Digital Forensics Analysis through a gamified satellite cybercrime scenario. The first part includes a series of five online 3D “escape rooms” which each simulate different locations that contain important evidence. After all the information is collected, participants enter the second phase of the challenge and begin conducting forensic analysis. Participants will respond to a fictional storyline where the flight control system of a Low Earth Orbit (LEO) is compromised. Due to the hack, the rocket and its accompanying satellite crash before reaching orbit. The software payload survives the crash and is sufficiently intact for digital forensic analysis. The participants act as cybersecurity digital forensics analysts, attempting to find out how and why the system was hacked and by whom. It is being deployed at the California Cyber Innovation Challenge 2020, the state championship for cybersecurity competitions in California, for teams of middle school and high school students this upcoming October.

Discord: <https://discord.com/channels/708208267699945503/732393009215176854>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Friday - 11:00-11:30 PDT

Title: Mission Kill: Process Targeting in ICS Attacks

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: ICS Vlg

SpeakerBio: Joe Slowik

Joe Slowik has experience across multiple facets of cyber and information operations stretching over 10 years. Past roles include operations planning and mission development within the US Department of Defense; planning network defense strategies for US Naval assets afloat; running incident response operations at Los Alamos National Laboratory; building a threat intelligence program within the US Department of Energy; critical infrastructure attack analysis and activity tracking; and assisting industrial control system asset owners and operators in defensive planning and response.

Twitter: [@jfslowik](#)

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - [ics Calendar file](#)

Title: MITM - The Mystery In The Middle. An Introduction To The Aircraft Information Systems Domain

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Aerospace Vlg

SpeakerBio: Matt Gaffney

Matt is an aviation cybersecurity consultant at BSSI UK where he also holds the position of Managing Director. He started his cybersecurity career whilst serving in the British Army after being volunteered for a mandatory IT Security Officer course because he 'has some experience with IT'. With more than 14 years experience across multiple industries from Military and Government to banking and aviation, Matt has mostly worked on the entry into service of e-Enabled aircraft at the operator (airline) level. Due to this, his focus is primarily on systems implemented by the operator and whose touchpoints are the Aircraft Information Systems Domain (AISD). His particular areas of interest are the Electronic Flight Bag (EFB) and ground systems. A relative newbie to the research field, he recently released his first paper 'Securing e-Enabled aircraft information systems' and plans on releasing others in the coming months.

Description:

The modern e-Enabled aircraft is often described as a flying data center with half of it on the ground. Sometimes overlooked by researchers in favour of avionics and In-Flight Entertainment systems, this presentation will give an introduction to the Aircraft Information Systems Domain (AISD). This hidden yet important domain logically sits between the Avionics and the passenger network and operators need to consider security in the AISD when bringing e-Enabled aircraft in to their fleet.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Saturday - 13:30-13:59 PDT

Title: MITRE ICS ATT&CK

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: ICS Vlg

Speakers: Marie, Otis

SpeakerBio: Marie

No BIO available

SpeakerBio: Otis

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 10:00-10:30 PDT

Title: ML Security Evasion Competition 2020

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: AI Vlg

Speakers:drhyrum,zh4ck

SpeakerBio:drhyrum

No BIO available

Twitter: [@drhyrum](#)

SpeakerBio:zh4ck

No BIO available

Twitter: [@zh4ck](#)

Description:No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DL - Friday - 12:00-13:50 PDT

Title: Mobile Security Framework - MobSF

When: Friday, Aug 7, 12:00 - 13:50 PDT

Where: See Description or Village

SpeakerBio: Ajin Abraham

Ajin Abraham is a Security Engineer with 7+ years of experience in Application Security and Offensive Security Research. He is passionate on developing new and unique security tools. Some of his contributions to Hacker's arsenal include OWASP Xenotix XSS Exploit Framework, Mobile Security Framework (MobSF), Droid Application Fuzz Framework (DAFF), NodeJsScan etc to name a few. He has been invited to speak at multiple security conferences including ClubHack, Nullcon, OWASP AppSec Eu, OWASP AppSec AsiaPac, BlackHat Europe, Hackmiami, Confidence, BlackHat US, BlackHat Asia, ToorCon, Ground Zero Summit, Hack In Paris, Hack In the Box, c0c0n and PHDays.

Description:

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

Interact @ #dl-ajin-mobile-securit-framework-text: <https://discord.com/channels/708208267699945503/730256193683062825>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://mobsf.github.io/Mobile-Security-Framework-MobSF/>

Forum: <https://forum.defcon.org/node/233122>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Sunday - 10:10-10:59 PDT

Title: Modeling systematic threat: testing on mainnet fork

When: Sunday, Aug 9, 10:10 - 10:59 PDT

Where: Blockchain Vlg

SpeakerBio: Martinet Lee

No BIO available

Description: No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ETV - Friday - 14:00-14:59 PDT

Title: Models of Privacy Norms

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Ethics VIg

Speakers:R. Jason Cronk,Ece Gumusel

SpeakerBio:R. Jason Cronk

No BIO available

SpeakerBio:Ece Gumusel

No BIO available

Description:

This will be a live talk.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Modern Red Team Tradecraft - Informing Defenders by Evolving Your Attackers

When: Saturday, Aug 8, 02:15 - 03:15 PDT

Where: Red Team VIg

SpeakerBio: Sajal Thomas

Sajal Thomas is a Senior Consultant at FireEye Mandiant. He works with the Mandiant Red Team in the Asia Pacific region. Sajal has simulated adversaries and helped secure customers in India, Singapore, Malaysia, Thailand, Japan, Indonesia, Philippines, Hong Kong, Taiwan, Australia, New Zealand, United Kingdom, Germany and the United States which provides him a unique insight into the diverse landscape of the challenges faced by attackers and defenders. In his free time, Sajal enjoys brewing coffee, watching football and reading about nation-state cyber espionage tradecraft.

Description:

Modern attacks against complex network infrastructure highlight a massive gap between state-affiliated cyber espionage attacks and Red Teams. As Red Teams face challenges that real-world attackers do not, replicating the sophisticated threat groups becomes all the more challenging with tight engagement deadlines and report submissions. The talk aims to bridge this gap by providing insights into modern tradecraft employed by the apex predators as well as the coin-miners and ransomware authors. The talk will also discuss the unique relationship between speed and stealth during Red Team operations. Sometimes "speed is the new stealth" but with evolved defensive technologies that baseline behaviour of endpoints on the host and network level, slow and steady may be the way to go instead. Additionally, the talk will walk through publicly-known implant design considerations to defeat mature host and network defences. Bleeding-edge credential harvesting techniques and the evolution of running Invoke-Mimikatz.ps1 to digging deep into C/C++ and Win32 API programming will be featured. Lastly, the evolution of a modern Red Team operator/developer/both will be discussed. The skills and mindset required to successfully complete objectives and evade defences have changed over time. A Red Teamer must evolve to be able to inform defence better.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Friday - 15:30-15:59 PDT

Title: Monero Wallet Basics: Sending, Receiving, Proving

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: Monero Vlg

SpeakerBio:rehr

No BIO available

Description:No Description available

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Saturday - 14:00-14:59 PDT

Title: Monetary Maximalism and Millennial Finance - Building Decentralized Tooling to Empower Everyone

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Blockchain Vlg

Speakers:Kris Jones,Matt Luongo

SpeakerBio:Kris Jones

No BIO available

SpeakerBio:Matt Luongo

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

DC - Saturday - 20:00-21:59 PDT

Title: Movie Stream - Lost World

When: Saturday, Aug 8, 20:00 - 21:59 PDT

Where: See Description or Village

Description:

'The Lost World' - Like Jurassic park but with title cards. Silent Film era, with dinosaurs. From 1925.

Banter @ #movie-night-text: <https://discord.com/channels/708208267699945503/741067993617924227>

Watch @ #movie-night-voice: <https://discord.com/channels/708208267699945503/741068040132624505>

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOT - Friday - 15:15-16:15 PDT

Title: NAND Flash – Recovering File Systems from Extracted Data

When: Friday, Aug 7, 15:15 - 16:15 PDT

Where: IOT Vlg

Description:

This learning session will introduce attendees to the process of recovering file systems from data extracted from NAND flash chips. As part of this learning session we will be discussing and demoing the tools, methods and common processes for successfully recovering data. After each learning objective we will have Q&A sessions

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: National Service Panel: Career Opportunities Supporting the Country

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: Career Hacking Vlg

Speakers: John Felker, Diane Janosek, Chris Pimlott, Roman Vitkovitsky, Liz Popiak, Joe Billingsley

SpeakerBio: John Felker , Assistant Director of the DHS Cybersecurity and Infrastructure Security Agency (CISA)

No BIO available

<https://www.linkedin.com/in/jofelker/>

SpeakerBio: Diane Janosek , Commandant of the NSA's National Cryptologic School and President of the Women in Cybersecurity Mid-Atlantic Affiliate

No BIO available

<https://www.linkedin.com/in/diane-janosek-abc/>

SpeakerBio: Chris Pimlott , Engineer at the US Digital Service

No BIO available

<https://www.linkedin.com/in/pimlottc/>

SpeakerBio: Roman Vitkovitsky , US Marine Marine Corps Cyber Auxiliari

No BIO available

<https://www.linkedin.com/in/rvitko/>

SpeakerBio: Liz Popiak

Created the US Army Cyber Speciality Direct Commissioning Program

<https://www.linkedin.com/in/elizabeth-popiak-mba-881a4b16/>

SpeakerBio: Joe Billingsley , Founder of the Military Cyber Professionals Association

No BIO available

<https://www.linkedin.com/in/joebillingsley/>

Description:

The National Service Panel highlights the opportunities and challenges with national service, focusing on tech-related programs across the federal government. The panel is organized by the Military Cyber Professionals Association (MCPA) and includes reps discussing the US Digital Service, US Marine Corps Cyber Auxiliary, National Security Agency (NSA), US Army Cyber Direct Commissioning Program, and Cybersecurity and Infrastructure Security Agency (CISA).

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

Return to Index - Add to  - ics [Calendar](#) file

Title: Next level stalker ware

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Cecilie Wian

Cecilie wian has a background in psychology and healthcare. She holds a BA in Educational psychology and a MA in Philosophy of technology. Her human-centric approach to software testing and development challenges established ways of creating systems meant for end-users.

Description:

What if parents could see everything their children had ever purchased? What if your ex could get a list of all your expenses? Without you knowing, or using the service yourself? It's already happening because many companies allow this kind of spying with nothing more than a person's bank card number, account number or license plate number.

Norway is far ahead in adoption of digital solutions. Services, bank services, and citizenship. Automatic detection of license plates, and digital receipt. Now the dark side of this is revealed: several cases of the next level stalker ware. Where bad actors gain access to other peoples information via centralized services, using easily obtainable, pieces of information.

Even when made aware of the problem the companies choose to accept the risk, pushing the responsibility and cost to stay safe on to the unknowing users. But what can we do ?

The talk will describe the process of pursuing some of the cases in a country with GDPR implemented, as well as discuss efforts to provide non-users with additional security and privacy.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ENT - Friday - 22:00-22:59 PDT

Title: Ninjula

When: Friday, Aug 7, 22:00 - 22:59 PDT

Where: See Description or Village

Description:

#1 DJ in my mothers eyes

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Facebook: <https://facebook.com/countninjula>

Twitter: <https://twitter.com/countninjula>

Soundcloud: <https://soundcloud.com/ninjula>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: No Question: Teamviewer, Police and Consequence (Beginner)

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio:corvusactual

Bill Dungey is a media maker, infoholic and professional nerd. Grab his latest work from postpunksuperhero.com.

Twitter: [@corvusactual](https://twitter.com/corvusactual)

<https://postpunksuperhero.com>

Description:

In the summer of 2019, I attended DEFCON for the first time and spent my days lingering around the Blue Team Village. Two weeks after I returned, our largest client was breached. A malicious actor remotely installed keyloggers on over a hundred computers.

After a marathon of logs and OSINT, I traced the bad guy to his house. I offered a dossier with everything I'd found to the local Cyber Crime unit, leading to a full confession and finally, the release of the suspect for circumstances I'm not authorized to know.

This talk discusses an internal breach of a non-profit organization. A delicate mix of politics, technical challenge and pressure, this event fundamentally shifted my career.

A strange log file triggered a closer look at some servers. Within minutes, we had realized a massive breach had taken place.

We found a keylogger installed on over a hundred computers. After a little digging, we found an unknown username referenced in a handful of Teamviewer connection logs.

Teamviewer was uninterested in helping us without an international warrant of some kind. Through a day of parsing log files (no, we don't have SIEM, IDS or IPS at this client), OSINT and the confidence I'd gained from finding a tribe at the BTV, I was able to identify the person responsible and gain insight into a real-world breach.

A search warrant was executed, devices were nabbed for forensics and the detective secured a full confession. I was told there was 'No Question', this was the person responsible, a client from the very organization that had been hit.

Some time later, after some political meetings between the parties involved, it was determined that a charge would not be levied against the malicious actor for reasons I have yet to be told. The organization is still actively under attack via weekly spear-phishing and whaling. After six weeks, the organization allowed the confirmed suspect back into the fold, accessing programs within the umbrella of the agency and within reach of the very systems he used to gain his foothold.

This is a vital topic to Blue Teamers. The real-world implications of a breach aren't clear or fair and it's all up to you.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: No Tech Talks

When: Saturday, Aug 8, 18:00 - 19:59 PDT

Where: See Description or Village

Description:

No tech? No problem. Come tell your no-tech stories here. It's like karaoke, except without the music, or cheesy lyrics, or singing. OK, it's not exactly like karaoke but it'll still be entertaining. Suggested theme: "Discovery" and "Apocalypse"

Selected speakers will get 15 minutes to tell their stories on the Discord voice channel, and audience members will be able to ask questions, or discuss on the text channel.

The sign up form won't be open until the night of the event, participation will be first come first serve, and subject to moderation.

Sign Up: <https://forms.gle/HX2Ujfgm5B9tP39H7>

#war-story-and-no-tech-talk-voice: <https://discord.com/channels/708208267699945503/733562286572306492>

#war-story-and-no-tech-talk-text: <https://discord.com/channels/708208267699945503/733562098315034735>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Nyan Sat Workshop

When: Friday, Aug 7, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

What's another way to hack a satellite? Through ground stations.

Nyansat consists of three fun, non-competitive challenges: building your own satellite tracking antenna, exploiting a ground station modem, and participating in our livestreamed, internet-accessible, community ground station event.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Nyan Sat Workshop

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: Aerospace VIg Workshop

Description:

What's another way to hack a satellite? Through ground stations.

Nyansat consists of three fun, non-competitive challenges: building your own satellite tracking antenna, exploiting a ground station modem, and participating in our livestreamed, internet-accessible, community ground station event.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Nyan Sat Workshop

When: Sunday, Aug 9, 09:00 - 13:59 PDT

Where: Aerospace VIg Workshop

Description:

What's another way to hack a satellite? Through ground stations.

Nyansat consists of three fun, non-competitive challenges: building your own satellite tracking antenna, exploiting a ground station modem, and participating in our livestreamed, internet-accessible, community ground station event.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: O365Squatting (Intermediate)

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: Blue Team Vlg - Talks Track 1

Speakers: Juan Francisco, Jose Miguel Gómez-Casero Marichal

SpeakerBio: Juan Francisco

Juan Francisco Bolivar is Chief Security Envoy at ElevenPaths and IT Security Manager on Pharma Industry, involved on security researching since more than 10 years, web, mobile applications and Industrial systems. His main focus is Industrial security critical infrastructures. He has recently published the first book in Spanish about Industrial security,

<https://0xword.com/es/libros/85-infraestructuras-criticas-y-sistemas-industriales-auditorias-de-seguridad-y-fortificacion.html>.

Previously he has been working as pentester and security engineer for international companies, releasing more than 10 0-days for vendors as Cisco, Honeywell, Siemens.... His is teaching at several university masters in Spain and South-America and public speaking on different security conferences Vicon, Hackron, TizonaConf, Honeycon, Isaca...

Twitter: [@jfran_cbit](https://twitter.com/jfran_cbit)

SpeakerBio: Jose Miguel Gómez-Casero Marichal

No BIO available

Description:

O365Squatting is a python tool created to identify that domains before the attack start. The tool can create a list of typo squatted domains based on the domain provided by the user and check all the domains against O365 infrastructure, (these domains will not appear on a DNS request).

At the same time, this tool can also be used by red teams and bug bunters, one of the classic attacks is the domain takeover so, the second option of this too is to check if the domain is registered in O365 in order to launch a domain takeover attack.

One of the main benefits of cloud technology is to deploy quickly services, with minimum interaction from the administrator side, this is an advantage exploited by cyber criminals too. Nowadays the main threats all size companies are facing is phishing, every day cyber criminals are creating more sophisticated techniques to cheat users and make more difficult the job of blue teams. The most common technique used is typo squatting. Part of the Blue team mission is to detect phishing, typo squatters, and attack domains before the phishing campaign begins, there is outside plenty of tools trying to detect that domains based on DNS, however none of them are focus into the cloud.

O365Squatting is an OpenSource tool created on Pyhton3, that can be launched automatically using cron. This is a unique tool, not only because of the cloud capabilities, if not because is prepared to be integrated with commercial SIEM as ArcSight based on the output possibilities, on screen or in format CEF and JSON.

When you create an account into O365 you can get a domain to use on your server mail on O365, however this domain is not published into DNS servers. Not publishing the domain automatically as AWS or GCloud is doing create a serious problem for organizations and blue team keeping a grey area for monitoring of domains. Our team has detected 100's of attacks using this method that classic tools are not detecting O365Squatting runs locally without sharing any info allowing:

Create list of squatted domains

Check squatted domains on O365

Check possible domain takeover on O365 Export in several formats (CEF, JSON)

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

CHV - Friday - 11:00-11:50 PDT

Title: OBD and what we CAN do with it

When: Friday, Aug 7, 11:00 - 11:50 PDT

Where: Car Hacking Vlg 101

SpeakerBio:Infenet

Lifelong hacker and hacker of all the things. Founder of Enterprise Offensive Security, creator of security tools for DevOps Engineers such as auto-remediation using AWS Lambda and CIS Compliance Scanning Tools, SSO implementations on the Service Provider and Identity Provider side(s). Simulated Advanced Persistent Threat Actor. Started DEFCON group in Detroit DC313 and Director of #misc Detroit.

Description:

Learn about the history of on-board diagnostics, OBD I and II Standards, Data Is Accessible From the OBD II and Architecture of OBD-II and CAN.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OBD and what we CAN do with it

When: Saturday, Aug 8, 11:00 - 11:50 PDT

Where: Car Hacking VIg 101

SpeakerBio:Infenet

Lifelong hacker and hacker of all the things. Founder of Enterprise Offensive Security, creator of security tools for DevOps Engineers such as auto-remediation using AWS Lambda and CIS Compliance Scanning Tools, SSO implementations on the Service Provider and Identity Provider side(s). Simulated Advanced Persistent Threat Actor. Started DEFCON group in Detroit DC313 and Director of #misc Detroit.

Description:

Learn about the history of on-board diagnostics, OBD I and II Standards, Data Is Accessible From the OBD II and Architecture of OBD-II and CAN.

#chv-101-talks-text: <https://discord.com/channels/708208267699945503/735651343007744051>

YouTube: https://www.youtube.com/watch?v=N4y_K4GGsLs

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Offensive Embedded Exploitation : Getting hands dirty with IOT/Embedded Device Security Testing

When: Thursday, Aug 6, 23:00 - 23:59 PDT

Where: Red Team Vlg

SpeakerBio: Kaustubh Padwad

Kaustubh is a Product security Assurance Manager at Reliance Jio Platform limited, his main work include Securing JIO's Cutting Edge Enterprise, Consumer, and SMB(small,Medium,Big) business products. His main area of interest is Device security,Reverse engineering, discovering RCE,Priv-esc bugs in proprietary or close source devices. He was Null champion, He had deliver more than dozens of talk in null meet and he was champion for 3 years in null community. Also he was a speaker at Owasp SeaSide 2020,Bsides Boston 2020. Some of his works are published in SecurityWeek, ExploitDB, Oday.today and have more than Dozens of CVE, Recently he was the winner of SCADA CTF @ nullcon 2019.

Description:

The world is moving towards smart culture everything nowadays is smart, and mostly all are those smart devices are basically embedded devices with internet connectivity or some provision to connect with the internet. Since these devices are booming in market this also tempting lots of people/groups for hacking. In this 1 hour talk we will discuss how to test the embedded/IoT devices, it would give you a methodology for assessment, how to perform firmware analysis, identifying vulnerable components, basic approach for reverse engineering the binaries to discover potential remote code execution, memory corruption vulnerabilities by looking for native vulnerable functions in C or bad implementation of functions like System, popen, pclose etc. After conducting static analysis, firmware analysis we will move towards dynamic testing approach which include web application testing, Underlying OS security testing, identifying vulnerabilities and misconfiguration in device. At last we will move towards fuzzing the device via web application parameters and installing appropriate debugger on device to identify memory corruption vulnerabilities.

DELIVERABLES

Methodology for testing embedded devices Deep dive into device security testing from beginner level to developing exploit And At last, a good intro into how to break known security boundary of embedded/IoT devices by knowing its weakness and thereby securing it.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Office Drama on macOS

When: Friday, Aug 7, 18:30 - 18:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Patrick Wardle , Principal Security Researcher

Patrick Wardle is the Principal Security Researcher at Jamf and founder of Objective-See. Having worked at NASA and the NSA, as well as presented at countless security conferences, he is intimately familiar with aliens, spies, and talking nerdy. Patrick is passionate about all things related to macOS security and thus spends his days finding Apple 0days, analyzing macOS malware and writing free open-source security tools to protect Mac users.

Twitter: [@Jamf](#)

Description:

On the Windows platform, macro-based Office attacks are well understood (and frankly are rather old news). However on macOS, though such attacks are growing in popularity and are quite en vogue, they have received far less attention from the research and security community.

In this talk, we will begin by analyzing recent documents that contain macro-based attacks targeting Apple's desktop OS, highlighting the macOS-specific exploit code and payloads. Though sophisticated APT groups are behind several of these attacks, (luckily) these malicious documents and their payloads are constrained by recent application and OS-level security mechanisms.

However, things could be far worse! To illustrate this claim, we'll detail the creation of a powerful exploit chain, that begins with CVE-2019-1457, leveraged a new sandbox escape and ended with a full bypass of Apple's stringent notarization requirements. Triggered by simply opening a malicious (macro-laced) Office document, no other user interaction was required in order to persistently infect even a fully-patched macOS Catalina system!

To end the talk, we'll discuss various prevention and detection mechanisms that could thwart each stage of the exploit chain, as well as that aim to generically provide protection against future attacks!

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Friday - 12:30-13:30 PDT

Title: On the insecure nature of turbine control systems in power generation

When: Friday, Aug 7, 12:30 - 13:30 PDT

Where: ICS Vlg

Speakers:Alexander Korotin,Radu Motspan

SpeakerBio:Alexander Korotin

Alexander Korotin is ICS security specialist at Kaspresky, focused on ICS security assessment, analysis of industrial software and protocols and penetration testing. At his previous job at Russian Railway Cybersecurity Center Alexander was involved in the security research of the railway transportation systems. Alexander has over five years of experience in this field. He is also OSCP certified.

SpeakerBio:Radu Motspan

No BIO available

Description:No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

Return to Index - Add to  - ics [Calendar](#) file

Title: onkeypress=hack();

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: Hardware Hacking Vlg

Speakers: Farith Pérez Sáez, Luis Ángel Ramírez Mendoza (@larm182luis), Mauro Cáseres

SpeakerBio: Farith Pérez Sáez

Farith Pérez Sáez (@f_perezs) is a colombian engineer, hardware hacker and speaker. He spoke at DragonJAR Colombia (Biggest hacking spanish speaking conference in LATAM) and teaches at Universidad de La Guajira.

Twitter: [@f_perezs](https://twitter.com/f_perezs)

SpeakerBio: Luis Ángel Ramírez Mendoza (@larm182luis)

Luis Ángel Ramírez Mendoza (@larm182luis) is a colombian electronic engineer, hacker and speaker. He spoke at DragonJAR Colombia (Biggest hacking spanish speaking conference in LATAM) and is currently working as a Cybersecurity and Artificial Intelligence Professor at University of Guajira in Colombia.

Twitter: [@larm182luis](https://twitter.com/larm182luis)

SpeakerBio: Mauro Cáseres

Mauro Cáseres (@mauroeldritch) is an argentine hacker and speaker. He spoke at DEF CON 26 Las Vegas (Recon & Data Duplication Villages), DevFest Siberia, DragonJAR Colombia, Roadsec Brasil, and DC7831 Nizhny Novgorod. Currently working as SecOps for the Argentine Ministry of Production.

Twitter: [@mauroeldritch](https://twitter.com/mauroeldritch)

Description:

In this talk we will see the assembly and use of a modified BadUSB keyboard with an integrated DIY physical keylogger. Using a built-in WiFi module, this keyboard is capable of sending user keystrokes to a remote server and storing it in a database. Both the piece by piece assembly, its diagram, and its programming will be demonstrated. Also there will also be a live demo to demonstrate its operation.

This talk is recommended for both novice and experienced users alike.

#hhv-onkeypresshack-talk-qa-text: <https://discord.com/channels/708208267699945503/736750677128249360>

Twitch: <https://twitch.tv/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: onkeypress=hack();

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: Hardware Hacking Vlg

Speakers: Farith Pérez Sáez, Luis Ángel Ramírez Mendoza (@larm182luis), Mauro Cáseres

SpeakerBio: Farith Pérez Sáez

Farith Pérez Sáez (@f_perezs) is a colombian engineer, hardware hacker and speaker. He spoke at DragonJAR Colombia (Biggest hacking spanish speaking conference in LATAM) and teaches at Universidad de La Guajira.

Twitter: [@f_perezs](https://twitter.com/f_perezs)

SpeakerBio: Luis Ángel Ramírez Mendoza (@larm182luis)

Luis Ángel Ramírez Mendoza (@larm182luis) is a colombian electronic engineer, hacker and speaker. He spoke at DragonJAR Colombia (Biggest hacking spanish speaking conference in LATAM) and is currently working as a Cybersecurity and Artificial Intelligence Professor at University of Guajira in Colombia.

Twitter: [@larm182luis](https://twitter.com/larm182luis)

SpeakerBio: Mauro Cáseres

Mauro Cáseres (@mauroeldritch) is an argentine hacker and speaker. He spoke at DEF CON 26 Las Vegas (Recon & Data Duplication Villages), DevFest Siberia, DragonJAR Colombia, Roadsec Brasil, and DC7831 Nizhny Novgorod. Currently working as SecOps for the Argentine Ministry of Production.

Twitter: [@mauroeldritch](https://twitter.com/mauroeldritch)

Description:

In this talk we will see the assembly and use of a modified BadUSB keyboard with an integrated DIY physical keylogger. Using a built-in WiFi module, this keyboard is capable of sending user keystrokes to a remote server and storing it in a database. Both the piece by piece assembly, its diagram, and its programming will be demonstrated. Also there will also be a live demo to demonstrate its operation.

This talk is recommended for both novice and experienced users alike.

#hhv-onkeypresshack-talk-qa-text: <https://discord.com/channels/708208267699945503/736750677128249360>

Twitter: <https://twitter.com/dchhv>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Online Ads as a Recon and Surveillance Tool

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Neil M

I am a member of the US Army and work in a cybersecurity-focused software development role. I am also an OSINT and online privacy enthusiast.

Description:

Inspired by and building on previous research and presentations on the topic (namely 0x200b's presentation from DEFCON 26*), this presentation will explore the possibility and feasibility of leveraging features of online targeted advertising platforms including Google and Facebook as a reconnaissance and surveillance tool. Unlike previous presentations at DEFCON, I intend to demonstrate that the targeted advertising attack has potential to be applied beyond the context of a red team targeting blue team personnel and can be leveraged against many average Internet users by a determined and resourced attacker. By exploring the advertising surveillance systems built into the majority of today's Internet-connected devices and services, I hope to enable privacy-conscious individuals to better protect themselves against targeted ad information collection schemes.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PAYV - Saturday - 11:00-11:59 PDT

Title: Online Banking Security

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: Payment Vlg

SpeakerBio: Arkadiy Litvinenko

No BIO available

Description:

Competition between banks leads to new opportunities for clients, which are the cause of new risks for the banks and for the clients themselves. During the talk we will discuss the internals of Online and Mobile banking, what vulnerabilities are common or specific for these services and what best practices exist for solving these problems.

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

Return to Index - Add to  - ics [Calendar](#) file

Title: Online MUD - EvilMog

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

This CTF is a MUD with 8-9 quests, intentional exploits, and about 1200 rooms has been setup at mog.ninja port 4000. A website documenting the MUD is at <https://mog.ninja> and a CTFd is setup at <https://ctf.mog.ninja>. The game is an LPMud and runs on gurbalib and DGD. If you complete all the quests you become a wizard. You connect by telnetting on port 4000. The game has been balanced out to take about a week to complete all the quests and hit max level if you find most of the in game exploits.

Forum: <https://forum.defcon.org/node/232895>

Discord: <https://discord.com/channels/708208267699945503/728707998796480590>

MUD Docs: <https://mog.ninja>

CTFd: <https://ctf.mog.ninja>

Return to Index - Add to  - ics [Calendar](#) file

Title: Online MUD - EvilMog

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

This CTF is a MUD with 8-9 quests, intentional exploits, and about 1200 rooms has been setup at mog.ninja port 4000. A website documenting the MUD is at <https://mog.ninja> and a CTFd is setup at <https://ctf.mog.ninja>. The game is an LPMud and runs on gurbalib and DGD. If you complete all the quests you become a wizard. You connect by telnetting on port 4000. The game has been balanced out to take about a week to complete all the quests and hit max level if you find most of the in game exploits.

Forum: <https://forum.defcon.org/node/232895>

Discord: <https://discord.com/channels/708208267699945503/728707998796480590>

MUD Docs: <https://mog.ninja>

CTFd: <https://ctf.mog.ninja>

Return to Index - Add to  - ics [Calendar](#) file

Title: Online MUD - EvilMog

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

This CTF is a MUD with 8-9 quests, intentional exploits, and about 1200 rooms has been setup at mog.ninja port 4000. A website documenting the MUD is at <https://mog.ninja> and a CTFd is setup at <https://ctf.mog.ninja>. The game is an LPMud and runs on gurbalib and DGD. If you complete all the quests you become a wizard. You connect by telnetting on port 4000. The game has been balanced out to take about a week to complete all the quests and hit max level if you find most of the in game exploits.

Forum: <https://forum.defcon.org/node/232895>

Discord: <https://discord.com/channels/708208267699945503/728707998796480590>

MUD Docs: <https://mog.ninja>

CTFd: <https://ctf.mog.ninja>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Online Voting: Theory and Practice

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: Crypto & Privacy Vlg

Speakers:Emily Stamm,Porter Adams

SpeakerBio:Emily Stamm

Emily Stamm is a security research engineer at Allstate specializing in cryptography. She graduated from Vassar college in 2018 with a degree in mathematics where she published original research papers in number theory. Her knowledge and interest in mathematics, quantum physics, and computer science motivated her passion for cryptography and quantum computing. Emily is also passionate about education and security awareness. She co-founded CyberSecurity Non-Profit (CSNP.org), an organization that provides free security educational resources, training, and events globally, with the purpose of making security more accessible, inclusive, and diverse.

SpeakerBio:Porter Adams

Porter Adams is a software engineer at Blacktop Government Solutions, co-founder of Disappear Digital, and member of CyberSecurity Non-Profit (CSNP). He loves cryptography, privacy, and protecting people online. He lives in Washington DC with his dog.

Description:

The concept of voting online is daunting to many because of the security risks, feasibility, and reliability. However, given the presence of election interference, limitations of in-person voting, and adoption of new technology, many countries are converting to electronic voting. In this talk, we discuss the theoretical and practical benefits and limitations of electronic voting. Emily Stamm will discuss the mathematics behind homomorphic encryption and blind signature schemes, with an emphasis on schemes that are secure against quantum computers. Porter Adams will discuss how these schemes and others are used in practice, and analyze the advantages and disadvantages of electronic voting.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

Return to Index - Add to  - ics [Calendar](#) file

Title: Only takes a Spark - Popping a shell on a 1000 nodes

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: ayoul3

Ayoub currently works as Lead Security at Qonto. He spent several years working as a pentester and an incident responder. He gave talks at various security conferences about Mainframe hacking. Lately, his main focus is Cloud security.

Twitter: [@ayoul3__](#)

Description:

Apache Spark is one of the major players if not the leader when it comes to distributed computing and processing. Want to use machine learning to build models and uncover fraud, make predictions, estimate future sales or calculate revenue ? Whip out a 200 nodes cluster on Spark and you are good to go.

This talk will show you how to get a shell on each one of these nodes! We are talking about systems that, by design, have access to almost every datastore in the company (S3, Cassandra, BigQuery, MySQL, Redshift, etc.). This is game over for most companies. I will also release a tool that will help pentesters pwn Spark clusters, execute code and even bypass authentication (CVE-2020-9480).

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ETV - Sunday - 14:00-14:59 PDT

Title: Open Live Chat for all Speakers or another talk on Ethics of Moderation

When: Sunday, Aug 9, 14:00 - 14:59 PDT

Where: Ethics VIg

SpeakerBio: Ethics Village Staff

No BIO available

Description:

This will be a live and open chat for everyone to participate in.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Saturday - 12:00-12:59 PDT

Title: Open Office Q&A w/ Monero Research Lab's Sarang

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Monero Vlg

SpeakerBio: Sarang

No BIO available

Description:

Ever wanted to have one of your Monero or cryptography related questions answered by the Monero Research Lab? Ask away!

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Open Ventilator Remote Monitoring Project

When: Sunday, Aug 9, 14:00 - 14:30 PDT

Where: BioHacking Vlg

Description:

2020 has been the year of COVID-19. The healthcare sector has been on the frontlines of battling this pandemic. There was significant projected demand for rapidly-manufactured ventilators during the early stages of the COVID-19 pandemic in the United States. Massachusetts was hard hit during the early stages of this pandemic, and the state's largest healthcare delivery organization brought together the open source community to develop new technologies and processes for rapidly developing resources needed to treat predicted growth of infections. The open source community came together to develop rapid prototype ventilators that could be potentially mass produced in quick succession. Many of these devices did not have built-in monitoring capabilities, so there was an anticipated need for staff to adequately track alarms in a centralized manner for these devices.

The Open Ventilator Monitoring Project addressed this need by rapidly creating a system that allows hospitals to monitor alarms and patient data from ventilators, integrating the status of multiple devices into a single display, similar to a central nursing station. During the design process of this project, an additional need was brought to the team's attention. Due to infection control procedures that require closing doors to patient rooms, clinical staff were unable to hear alarms from ventilators that were not already integrated into a traditional central monitoring system. The team then pivoted to develop a solution to modify the hardware and software system to include the ability to auditorily monitor and alert based on the sound pressure of these ventilator alarms.

To date, the team has delivered a Minimum Viable Product (MVP), which has undergone limited lab testing in the Massachusetts General Hospital's Medical Device Interoperability and Cybersecurity Program Lab (MGH MD PnP). The project has longer term goals of safety/integration, and ultimately, deployment within settings such as field hospitals. It is expected that this project's capabilities may be useful to many hospitals, extending beyond the constantly-changing emergency of COVID-19's spread.

This open source project is led by Sam Cervantes, MakerGear CTO and David Guffrey, MGB/Partners HealthCare Medical Device Cybersecurity Program Lead and includes ten contributors from the open source community, students, clinical engineers, and MITRE. The project utilizes both a cloud-based and embedded architecture, deployed on affordable & widely available consumer-grade hardware such as Raspberry Pi & Arduino. Software stacks used include Ruby on Rails, Javascript, Python, and C++.

While the software has been designed to monitor ventilators, the project's architecture - utilizing APIs and plugins - is extensible to other network environments and other device types.

Ultimately, hospitals in the U.S. have not experienced a shortage of traditional ventilators, and so our software was not needed during the Covid-19 crisis. However, we present a framework for rapidly developing software in crisis situations along with a set of lessons learned for those who follow in future crises.

In this talk, we will cover topics such as:

- The project's roots in remotely monitoring 3D printers;
- Current technical challenges, both solved and unsolved, such as the need for security and the pre-eminence of reliability;
- Special considerations required for IT developers entering into industries such as healthcare, where safety is paramount;
- The technical difficulties of implementing the project with constantly-evolving requirements;
- Lessons learned in the socio-technical challenges to adoption of such work, such as regulatory uncertainty with FDA's Emergency Use Authorization (EUA), finding corporate supporters and use cases, and moving beyond a minimum viable product.

- Lessons learned in product development during a crisis, such as the tradeoffs between deployment speed and stability
- Future developments / use-cases in broader sound-monitoring other medical devices (e.g. infusion pumps)
- Optional: live demo of hardware/software

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Open-Source Tools for Hunting and Practical Intelligence (Intermediate)

When: Friday, Aug 7, 16:30 - 17:59 PDT

Where: Blue Team VIg - Workshop Track 1

SpeakerBio: Joe Slowik

Joe Slowik has experience across multiple facets of cyber and information operations stretching over 10 years. Past roles include operations planning and mission development within the US Department of Defense; planning network defense strategies for US Naval assets afloat; running incident response operations at Los Alamos National Laboratory; building a threat intelligence program within the US Department of Energy; critical infrastructure attack analysis and activity tracking; and assisting industrial control system asset owners and operators in defensive planning and response.

Twitter: [@jfslowik](#)

Description:

Organizations need to identify and disposition new threats to ensure active, adaptive defense. This workshop will walk through open source resources and freely-available techniques to identify new threats and attack trends, and how to then formulate defensive strategies for enterprise protection.

Open source intelligence and information gathering Company blogs, articles, and media reporting Distinguishing between technical reporting and pure marketing "Reading between the lines" for search terms Social media and Twitter

Suggested accounts

Source vetting and evaluation

Public threat feeds: AlienVault, IBM X-Force Registration and data retrieval

Timeliness and value

Sample gathering and extracting information HybridAnalysis, ANY.RUN, MalShare, VirusShare – VT (commercial)
Capabilities and limitations of free services Evaluating different reporting types, extracting information for further searching
How to read an analysis or incident report More reading between the lines
Going beyond hashes and IPs

Extracting information for use and application

Formulating information into hypotheses and pivoting Network pivoting: DomainTools, RiskIQ, Censys, Shodan, Urlscan, VirusTotal (free) The art of network pivoting without going 'too far' Pivoting types: registration information, SOA leaks, infrastructure similarities, etc. Host/Binary pivoting: VirusTotal, HybridAnalysis, ANY.RUN, etc. File metadata and compilation artifacts

Identifying common tooling, techniques, and references to publicly-available projects

Overview and exercise:

Beginning with a single sample (malicious document file), extracting additional information Identifying items of interest in document, identifying payload Using information to identify general patterns, trends, and behaviors Translating identified information into rules, hunting hypotheses, and defensive measures Deliverable: Additional IOCs, brief report for review and feedback (after conclusion of workshop)

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON



DEFCON

DEFCON

Title: Opening Remarks: Getting The Aerospace Village To Take-Off

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Aerospace Vlg

Speakers:Chris Krebs,Dr Will Roper,Pete Cooper

SpeakerBio:Chris Krebs

Christopher Krebs - serves as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Mr. Krebs was originally sworn in on June 15, 2018 as the Under Secretary for the predecessor of CISA, the National Protection and Programs Directorate (NPPD). Mr. Krebs was nominated for that position by President Trump in February 2018.

Before serving as CISA Director, Mr. Krebs was appointed in August 2017 as the Assistant Secretary for Infrastructure Protection. In the absence of a permanent NPPD Under Secretary at the time, Mr. Krebs took on the role of serving as the Senior Official Performing the Duties of the Under Secretary for NPPD until he was subsequently nominated as the Under Secretary and confirmed by the Senate the following year.

Mr. Krebs joined DHS in March 2017, first serving as Senior Counselor to the Secretary, where he advised DHS leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. Prior to coming to DHS, he was a member of Microsoft's U.S. Government Affairs team as the Director for Cybersecurity Policy, where he led Microsoft's U.S. policy work on cybersecurity and technology issues.

Before Microsoft, Mr. Krebs advised industry and Federal, State, and local government customers on a range of cybersecurity and risk management issues. This is his second tour working at DHS, previously serving as the Senior Advisor to the Assistant Secretary for Infrastructure Protection and playing a formative role in a number of national and international risk management programs.

As Director, Mr. Krebs oversees CISA's efforts to defend civilian networks, manage systemic risk to National critical functions, and work with stakeholders to raise the security baseline of the Nation's cyber and physical infrastructure.

Mr. Krebs holds a bachelor's degree in environmental sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

SpeakerBio:Dr Will Roper

Dr. Will Roper - is the Assistant Secretary of the Air Force for Acquisition, Technology and Logistics. As the Air Force's Service Acquisition Executive, Dr. Roper is responsible for and oversees Air Force research, development and acquisition activities totaling an annual budget in excess of \$60 billion for more than 550 acquisition programs. In this position, Dr. Roper serves as the principal adviser to the Secretary and Chief of Staff of the Air Force for research and development, test, production and modernization efforts within the Air Force.

Prior to his current position, Dr. Roper was the founding Director of the Pentagon's Strategic Capabilities Office. Established in 2012, the SCO imagines new—often unexpected and game-changing—uses of existing government and commercial systems: extending their shelf- life and restoring surprise to the military's playbook. Since 2012, SCO has grown from an annual budget of \$50 million to the current \$1.5 billion request in the President's 2018 budget with projects spanning new concepts such as hypervelocity artillery, multi-purpose missiles, autonomous fast-boats, smartphone-navigating weapons, big-data- enabled sensing, 3D-printed systems, standoff arsenal planes, fighter avatars and fighter-dispersed swarming micro-drones which formed the world's then-largest swarm of 103 systems. During his tenure as SCO Director, Dr. Roper served on the Department's 2018 National Defense Strategy Steering Group, Cloud Executive Steering Group and Defense Modernization Team.

Previously, Dr. Roper served as the Acting Chief Architect at the Missile Defense Agency where he developed 11 new systems, including the current European Defense architecture, advanced drones, and classified programs. Before this, he worked at MIT Lincoln Laboratory and served as a missile defense advisor to the Under Secretary of Defense for Acquisition, Technology and Logistics.

SpeakerBio:Pete Cooper

Pete Cooper - Dir Aerospace Village. His first tech love was a ZX Spectrum but then he then moved on to flying fast jets in the UK Royal Air Force. Then he moved into cyber operations before leaving the military 4 years ago. Since then he has started up his own cyber security firm and has advised on everything from developing global cyber security strategies with UN bodies such as ICAO, advising the ICRC on the nature of state vs state cyber conflict and also enjoys playing with active cyber defence and deception. Pete is also the founder and Dir of the UK Cyber Strategy Challenge “Cyber9/12”, holds an MSc in Cyberspace Operations, is a Senior Fellow at Kings College London, a Non-Resident Senior Fellow at the Atlantic Council Cyber Statecraft Initiative and a Fellow of the Royal Aeronautical Society.

Description:

Let’s face it, relationships between the hacker / researcher community and the aerospace sector in the past – haven’t been great. 20 months ago, a passionate voluntary group of hackers, pilots, engineers, policy wonks and others, decided to do something about it and start creating a community that would foster trusted relationships across all those interested in aviation cyber security. Here we are at our second DEF CON in the Aerospace Village with a rapidly growing hacker / researcher community supported by the aerospace industry, USAF, DDS, CISA, academia, regulators and more including the first satellite CTF.

A short intro to the Aerospace Village tells the story of how and why we do this, how we got here and where we are going.

Then we are honoured to have two guest speakers where we hear from Dir CISA, Chris Krebs, who will be chatting about all things CISA and Aerospace Cybersecurity, after which things are rounded off by Dr Will Roper, Assistant Secretary of the Air Force for Acquisition, Technology and Logistics who will talk to the Space Security Challenge – Hack-a-Sat and their support for the Aerospace Village and its vision.

This event will be coordinated on the DEF CON Discord server, in channel #av-terminal-text.

Discord: <https://discord.com/channels/708208267699945503/732392946350948423>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 09:30-09:59 PDT

Title: Opening Remarks

When: Friday, Aug 7, 09:30 - 09:59 PDT

Where: AI Vlg

SpeakerBio: AI Village Organizers

No BIO available

Description: No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OpenSOC Blue Team CTF - Finals Round

When: Sunday, Aug 9, 09:00 - 11:59 PDT

Where: See Description or Village

Description:

OpenSOC is a Digital Forensics, Incident Response (DFIR), and Threat Hunting challenge meant to teach and test practical incident response skills in an environment that closely resembles a real enterprise network. This virtual environment is representative of what you would find in an enterprise network, including: workstations, servers, firewalls, email, web browsing, user activity, etc. Simulated users are browsing the Internet, downloading files, watching videos, and accessing LAN resources. This creates a high-fidelity training environment for unleashing real-world attacks and testing responders' abilities to filter and detect malicious activity on the network. This isn't just another CTF. We've built this platform to train real-world responders to handle real-world situations, and each year we incorporate new scenarios that are modeled after threat actors and breaches experienced by the OpenSOC team. From APT attacks using 0-days and heavily weaponized shellcode to sneaky lateral movement and exfiltration techniques, we expose contestants to a wide-range of techniques that we see actively used in the wild. We encourage team participation, and always have folks on hand to assist those just getting started out. Even better - 100% of the security tools demonstrated within OpenSOC are Free and/or Open Source! These projects include Velociraptor, Sysmon, osquery, Suricata, Moloch, pfSense and Graylog + ELK bringing it all together in an awesome way. This allows our contestants to not only have fun at DEF CON, but also learn skills and tools they can take back to work on Monday.

The Challenge:

- Given an initial IOC (indicator of compromise), identify attacks that are being carried out against and within the enterprise environment, pivoting between key artifacts
- Trace the attackers throughout the kill chain, submitting key IOCs and observables to the scoreboard as you reveal their tactics.
- Reverse engineer any artifacts connected to hostile activities.
- Perform forensics analysis on PCAPs (Packet Captures), memory images, etc.
- Win awesome prizes, learn new skills, and get experience with some of the best Open Source tools for SecOps!

Forum: <https://forum.defcon.org/node/232949>

Discord: <https://discord.com/channels/708208267699945503/711644213170667562>

Twitter: https://twitter.com/Recon_InfoSec

Web: <https://opensoc.io>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OpenSOC Blue Team CTF - General Round

When: Friday, Aug 7, 10:00 - 23:59 PDT

Where: See Description or Village

Description:

OpenSOC is a Digital Forensics, Incident Response (DFIR), and Threat Hunting challenge meant to teach and test practical incident response skills in an environment that closely resembles a real enterprise network. This virtual environment is representative of what you would find in an enterprise network, including: workstations, servers, firewalls, email, web browsing, user activity, etc. Simulated users are browsing the Internet, downloading files, watching videos, and accessing LAN resources. This creates a high-fidelity training environment for unleashing real-world attacks and testing responders' abilities to filter and detect malicious activity on the network. This isn't just another CTF. We've built this platform to train real-world responders to handle real-world situations, and each year we incorporate new scenarios that are modeled after threat actors and breaches experienced by the OpenSOC team. From APT attacks using 0-days and heavily weaponized shellcode to sneaky lateral movement and exfiltration techniques, we expose contestants to a wide-range of techniques that we see actively used in the wild. We encourage team participation, and always have folks on hand to assist those just getting started out. Even better - 100% of the security tools demonstrated within OpenSOC are Free and/or Open Source! These projects include Velociraptor, Sysmon, osquery, Suricata, Moloch, pfSense and Graylog + ELK bringing it all together in an awesome way. This allows our contestants to not only have fun at DEF CON, but also learn skills and tools they can take back to work on Monday.

The Challenge:

- Given an initial IOC (indicator of compromise), identify attacks that are being carried out against and within the enterprise environment, pivoting between key artifacts
- Trace the attackers throughout the kill chain, submitting key IOCs and observables to the scoreboard as you reveal their tactics.
- Reverse engineer any artifacts connected to hostile activities.
- Perform forensics analysis on PCAPs (Packet Captures), memory images, etc.
- Win awesome prizes, learn new skills, and get experience with some of the best Open Source tools for SecOps!

Forum: <https://forum.defcon.org/node/232949>

Discord: <https://discord.com/channels/708208267699945503/711644213170667562>

Twitter: https://twitter.com/Recon_InfoSec

Web: <https://opensoc.io>

Registration: <https://docs.google.com/document/d/1TbfOwv5C64ciirCQELq0HxJVd5oJd4qjvzXhidFgijw/edit?usp=sharing>

Return to Index - Add to  - ics [Calendar](#) file

Title: Operationalizing Cyber Norms: Critical Infrastructure Protection

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: ICS Vlg

SpeakerBio:Chris Kubecka

Chris Kubecka - "Fearless and powerful speaker, saves countries, fights cyber terrorism, advises several governments as a subject matter expert on cyber warfare national defense. Profiled by major media in the USA and Europe. USAF military combat veteran, former military aviator, and USAF Space Command. Defends critical infrastructure and handles country level cyber incidents, cyberwarfare, and cyber espionage. Reconnected Saudi Aramco international business operations & established digital security after the world's most devastating cyberwarfare attack. Developing the highest level of exploit code against IT/IOT/ICS SCADA control systems whilst working with governments. Involved in the world's biggest hacks, advising nations, NATO, Europol, Interpol exposing corruption and national security risks.

"She is a go-to professional for governments. There are only a certain number who can both frame the problem conceptually and put it in straight fuc**** English so somebody can understand. And she can do that.

Description:No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OSINTSECCryptoAIBlockchain

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231050>

Discord: <https://discord.com/channels/708208267699945503/732439527213367346>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: OSINTSECCryptoAIBlockchain

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231050>

Discord: <https://discord.com/channels/708208267699945503/732439527213367346>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: OSINTSECCryptoAIBlockchain

When: Sunday, Aug 9, 00:00 - 15:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231050>

Discord: <https://discord.com/channels/708208267699945503/732439527213367346>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Osquery: An Introduction Into OpenSOC CTF Tools

When: Thursday, Aug 6, 13:15 - 13:59 PDT

Where: Blue Team VIg - Workshop Track 1

SpeakerBio: Whitney Champion

Whitney is the lead architect at Recon InfoSec. In the last 15 years, she has worked on security, operations, support, development, and consulting teams, in both the private and public sector, supporting anywhere from a handful of users to hundreds of thousands. No matter the role, security has always been an area of passion and focus.

Twitter: [@shortxstack](#)

Description:

Learn. Play. Do.

Every year the Blue Team Village hosts OpenSOC. A unique defense CTF meant to teach and test practical incident response skills in an environment that's as close to "the real thing" as it gets.

This year BTV wanted to do more. We know that some Blue Teamers might be unfamiliar with some of the tools used by OpenSOC. And we didn't want that to keep anyone from playing this incredible defense simulation.

So this year we are dedicating all day Thursday to demo the various OpenSOC tools, before OpenSOC starts on Friday. These are tools like Graylog, Moloch, Zeek, Osquery, and others that Blue Teamers rely on every day to defend their networks against attackers.

That means that after you LEARN the tools, you can PLAY the OpenSOC CTF, and then take that knowledge back to your own Blue Team to DO the work of defending your network.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Saturday - 15:00-15:30 PDT

Title: OSTWERK Initiative

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: Ham Radio Vlg

Description:

OSTWERK stands for Open Source Tactical Wireless Emergency Radio Kit, an all-in-one customizable solution for building ham radio kits. This will be a 30 minute talk and Q&A about the initiative, my sample kit, and what I hope to accomplish (website features, sponsorships for kits for schools, etc). Feel free to ask any questions!

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: OU having a laugh?

When: Saturday, Aug 8, 04:45 - 05:45 PDT

Where: Red Team VIg

SpeakerBio:Petros Koutroumpis

Petros Koutroumpis is a security consultant and has delivered multiple red and purple team engagements. His research is mainly focused on Active Directory and Windows post-exploitation. He likes to spend his free time developing new tools and contributing to open-source projects.

Description:

Whether you are trying to attack or defend Active Directory, BloodHound has been the default tool for identifying attack paths. With its latest release, BloodHound3 has introduced a number of new edges including the collection of ACLs for Organizational Units.

In this talk we will present a method to abuse edit rights on an OU by serving malicious Group Policy Objects in order to compromise any computer or user object that is a member of the vulnerable OU or any of its child OUs.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Our journey into turning offsec mindset to developer's toolset

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: AppSec Vlg

Speakers:Paul Amar,Stanislas Molveau

SpeakerBio:Paul Amar

No BIO available

Twitter: [@PaulWebSec](#)

SpeakerBio:Stanislas Molveau

No BIO available

Description:No Description available

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: OuterHaven - The UEFI Memory Space Just Itching to be Misused (Intermediate)

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio: Connor Morley

A computer security obsessive, Connor has been a threat hunter for the past 3 years spending half his job time looking for vulnerabilities and ripping apart exploitation tools/malware. In addition to his investigative action, he also participates in enhancement and development of the industry leading detection system employed to actively detect and disrupt active attackers. Enjoying advanced attack methods, he has participated in active attack prevention and remediation as well as publishing white papers on APT level attack frameworks (Is Killswitch laying in wait? - Equation group) and tackling detection problems (Truecrypt detection and distributed attack system - TCrunch).

Twitter: @Lavi16

Description:

This presentation will cover research which explores the methods in which all levels of attackers can work with exploiting the UEFI memory space as well as methods for monitoring & enumerating this data haven and the associated access difficulties. I will also demonstrate some scripting and Python code that leverages Windows hosted elements to both exploit, enumerate and monitor this safe space for everyone to play with.

The exploitation of UEFI memory has previously only been thought of as something that is used for rootkits or advanced/targeted offensive operations. However, offensive actors and researchers have shown that they are willing to exploit this area with increasing ease. This presentation goes one step further and highlights the extremely basic level of computer knowledge needed to exploit this in current Windows OS, one-click and copy-paste scripts being able to generate the same results. However, the presentation also highlights solutions to monitor/access/analyze issues for this reclusive data set which allows active threats to be scrutinized and detection & preventative methods developed for both local and remote security solutions.

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Outs, Forces, and Equivoque: A treatise on how Magicians speak

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: Rogues Vlg

SpeakerBio: Brandon Martinez

No BIO available

Description:

In this talk, BM explores the similarities of language between both a magician and social engineer. Learn about common language tricks and methods used in magic and how those same methods could be used to make your social engineering more effective. After learning these principals, learn how to apply them them in ethical scenarios to help practice your skills, as well as having the tools to create new ones.

Rogues Village activities will be streamed via Twitch.

Twitch: <https://www.twitch.tv/roguesvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCG - Saturday - 10:00-10:59 PDT

Title: OWASP API Top 10

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: DEF CON Groups

Description:

Presentation by DC9111 (New Delhi, India)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

PHVT - Sunday - 11:00-11:59 PDT

Title: Packet Acquisition: Building the Haystack

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: Packet Hacking VIg - Talk

Speakers:Chris Abella,Pete Anderson

SpeakerBio:Chris Abella , P SE, ExtraHop Networks

No BIO available

SpeakerBio:Pete Anderson , Sr. SE, ExtraHop Networks

No BIO available

Description:

Packet hacking doesn't happen without packets. There are multiple methods to get packets from a network; from local tcpdump and Wireshark all the way to enterprise wide tapping and span aggregation. In this talk, we'll discuss enterprise packet acquisition strategies and challenges, and the methods, tools, and techniques necessary to build the data foundation for effective network-based detection and forensics.

Garbage data in means garbage analysis out. Chris and Pete have spent decades working with Fortune 500 NOC and SOC teams to implement advanced packet analysis solutions, build better packet pipelines, and get more from those packets.

YouTube: <http://youtube.com/wallofsheep>

Twitch: <http://twitch.tv/wallofsheep>

Facebook: <http://facebook.com/wallofsheep/>

Periscope: <https://t.co/gn17JLftA?amp=1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

IOT - Friday - 17:45-18:15 PDT

Title: Pandemic In Plaintext

When: Friday, Aug 7, 17:45 - 18:15 PDT

Where: IOT VIg

SpeakerBio: Troy Brown

Troy has been a RF and physical security hardware engineer for multiple manufacturers of access control, locks, and wireless security devices for over a decade. Troy holds multiple patents in areas of electronic security, energy harvesting, and wireless. Troy also hosts the YouTube channel for HackerWarehouse.TV and can be found on Twitter at @waveguyd.

Description:

When a wireless engineer decides to tune into hospitals to determine the state of COVID in the community, he finds detailed patient info being broadcast into thin air. By capturing, decoding, and analyzing the info, the true state of the pandemic is realized.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Panel: The Joy of Coordinating Vulnerability Disclosure

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: Red Team VIg

Speakers:Daniel Gruss,CRob,Lisa Bradley,Katie Noble,Omar Santos, Anders Fogh

SpeakerBio:Daniel Gruss , TU Graz

No BIO available

SpeakerBio:CRob , Red Hat

No BIO available

SpeakerBio:Lisa Bradley , Dell

No BIO available

SpeakerBio:Katie Noble , Intel Corp

Katie currently serves as a Director of PSIRT and Bug Bounty at Intel Corp. Where she leads the cyber security vulnerability Bug Bounty program, researcher outreach, and strategic planning efforts. Previous to this position, Katie served as the Section Chief of the Vulnerability Management and Coordination at the Department of Homeland Security, Cyber and Infrastructure Security Agency (CISA) where she led DHS' primary operations arm for coordinating the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems, enterprise, hardware and software. Katies team is credited by the Secretary of Homeland Security with the coordination and public disclosure of over 20,000 cyber security vulnerabilities within a two year period. Katie is a highly accomplished manager with over 14 years of U.S. Government experience, both in the Intelligence Community and Cyber Security Program Management. She has operated at all levels from individual contributor as an Intelligence Analyst for the National Intelligence Community to Senior Policy Advisor for White House led National Security Council (NSC) Cyber programs. Her work has directly impacted the decision making of the NSC, Defense Information Systems Agency, Office of the Director of National Intelligence, Department of Defense, Federal Communications Commission, Central Intelligence Agency, U.S. Coast Guard, U.K.Ministry of Defense, Canadian Government agencies, and Australian Cabinet Ministry.

SpeakerBio:Omar Santos , Cisco

Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure. Omar is the author of over 20 books and video courses; numerous white papers, and other articles. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities. Omar is often presenting at many conferences and he is the co-lead of the DEF CON Red Team Village.

Twitter: [@santosomar](https://twitter.com/santosomar)

SpeakerBio: Anders Fogh , Intel

No BIO available

Description:

Under the best of circumstances, coordinating disclosure of vulnerabilities can be a challenge. At times it can feel like everyone involved in CVD has conflicting motivations. The truth is that all of us are aspiring to do the right thing for end-users based on our perspective. The panel will share experiences and show how researchers and technology companies can work together to improve the impact of disclosing vulnerabilities on the technology ecosystem. Join CRob (Red Hat), Lisa Bradley (Dell), Katie Noble (Intel), Omar Santos (Cisco), Anders Fogh (Intel) and Daniel Gruss (TU Graz) for an exciting and engaging dialog between security researchers and industry experts on the Joy of coordinating vulnerability disclosure.

Presentation Outline

This will be an interactive session between the panelists. The following questions are seeds for what will be a dynamic and lively discussion: What does CVD mean to you and what is your motivation to disclose? What benefits have the panelists seen in coordinating vulnerability disclosure? What problems have you had with CVD? How does CVD work in open source projects? How do you prepare for coordinated vulnerability disclosure and what challenges do you face? How could researchers and industries work better together?

Takeaways

Learn about the exciting world of Coordinated Vulnerability Disclosure. Hear from experts from both the research community as well as the vendors they report issues to. Learn from the coordination mistakes from the past to not repeat them in the future. Learn about the current struggles with CVD and what needs to be done to improve CVD.

Problem to solve

The hope is that this constructive interaction will remove some of the impediments of relationships between product developers and security researchers. The goal is to open a door for dialogue that will bring more stability in the experiences we all have in coordinating vulnerability disclosure. All technology users are impacted by security vulnerabilities, how those issues are communicated and dealt with are critical to impacted individuals and organizations to effectively manage the information security risk. The panel hopes to show "both sides" of the issue and highlight our different perspectives, and ideally showcase we're all working to help secure end-users around the globe.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Password cracking beyond 15 characters and under \$500

When: Friday, Aug 7, 19:15 - 20:15 PDT

Where: Red Team VIg

SpeakerBio: Travis Palmer

Travis Palmer is a Red Team Engineer at Intercontinental Exchange and a certified OSCP and OSCE. Most recently he has been a "surprise" backup speaker at DEFCON 27, DEFCON Red Team Village Staff, and a speaker at Wild West Hacking Fest and Cisco Offensive Summit. He is a fan (and sometimes-contributor) of a number of simulator/sandbox video games, and keeper of too many unfinished hardware projects. In his video games he enjoys long assaults on the beach, and dancing jets in the rain.

Description:

Most of us understand that it is a good idea to tailor an attack to a password policy. That being said, most password policies are fairly homogeneous. Does a minimum eight characters and at least three of four categories for complexity sound familiar? The hashcat-herders among us have prepared well for this endeavor. Many have hoarded hundreds of gigabytes of dumped passwords from hacked sites using these exact kinds of policies. Which means, when the hashes get dumped, sometimes more than half of a domain can be cracked in a single day. So... what if you have to crack passwords written under a different policy, like a paranoid 15 character minimum? Those gigabytes of dictionaries, full of shorter passwords, aren't going to rockyou into domain admin anymore. It's time to dive into the hashes with combinations of combinator, purple rain attacks, and word-level linguistically correct Markov chains. Along with the techniques themselves, this presentation will include the real-world results of various cracking attacks against a ~6000 person domain, at a Fortune 500 with a mature security program. As well as some recommendations for policies that allow memorable passwords while actually making them difficult to crack.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Saturday - 00:00-00:59 PDT

Title: PathWell: Dynamic Password Strength Enforcement (Rebroadcast)

When: Saturday, Aug 8, 00:00 - 00:59 PDT

Where: Password Vlg

SpeakerBio: Hank Leininger

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Saturday - 13:00-13:59 PDT

Title: PathWell: Dynamic Password Strength Enforcement

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: Password Vlg

SpeakerBio: Hank Leininger

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: PatrOwl - Red flavour of SOC automation

When: Sunday, Aug 9, 01:00 - 01:59 PDT

Where: Red Team Vlg

SpeakerBio:Nicolas MATTIOCCO

Nicolas MATTIOCCO is an information security expert since 12 years and was involved in various security consulting engagements from penetration tests to global risk assessments and security operations implementation. Today, he is working as a red teamer and in automating security operations at a large scale.

Description:

A company, regardless of its size and market power, may go out of business or lose a lot of value because of a security incident on its information system. The number of vulnerabilities and the interest of cyber-attackers is only increasing. With the advent of the monetization of botnet cyber attacks or the installation of crypto-miners for example, the threats are going more varied and intensified, but less targeted. The vast majority of companies are digital and increasingly exposed on the Internet. The level of cyber exposure is also higher. The "Cyber" risk has become vital. Today, everything has changed and tomorrow everything will change even faster. Where manual analysis was sufficient, paradigms of risk assessment are moving towards more automation. But ****we need intelligent automation****.

This automation strategy also tends to address the drastic lack of competent cyber security resources and retention of talents. The automation of recurrent, time-consuming and low-value-added tasks will allow teams to focus on more complex and therefore more motivating topics. To efficiently support this strategy, we developed PatrOwl, an Open Source, Free and Scalable Security Operations Orchestration Platform. Technically, PatrOwl is a solution for automating calls to commercial or open source tools that perform checks. To date, more than 140 tools or online services are supported. Beyond centralizing the results (vulnerabilities, meta-data, asset metadata) obtained, the PatrOwl analysis engine compares these results with its knowledge base and other third-party services to determine scenarios of attacks (predictive analysis) or to trigger actions (alerting, program calls, ...). Largely customizable, PatrOwl is suitable for supporting penetration testing, vulnerability audit and compliance, static source audit, threat research (CTI) and security incident response activities (SOC / DFIR).

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Peeling Back the Layers and Peering Through the Clouds with Security Onion

When: Friday, Aug 7, 14:10 - 16:30 PDT

Where: Cloud Vlg

SpeakerBio: Wes Lambert

Wes Lambert is a Senior Engineer at Security Onion Solutions, where he helps companies to implement enterprise security monitoring solutions and better understand their computer networks. Wes is a huge fan of open source software projects, and loves to solve problems and enhance organizational security using completely free and easily deploy-able tools.

Twitter: [@therealwlambert](https://twitter.com/therealwlambert)

Description:

Peeling Back the Layers and Peering Through the Clouds with Security Onion As the number of production assets and workloads transition to cloud, it is more important than ever to be able to understand the "goings-on" of these type of environments. Unfortunately, many organizations still have little visibility into cloud infrastructure. Vendor-specific solutions can be cost-prohibitive, and don't always offer a complete solution for security monitoring. In this session, we'll discuss how we can better defend cloud environments by leveraging Security Onion, a completely free and open source platform for intrusion detection, enterprise security monitoring, and log management. By using Security Onion, we can pierce the veil of the cloud, and gain better visibility to facilitate threat detection, identify application misconfigurations, and assist with compliance-related efforts. Attendees should walk away with a firm grasp of the platform, understanding how they can utilize Security Onion to improve their organization's security posture, and make their adversaries cry.

Outline

- (1) Cloud
 - (a) Assets/Data
 - (b) Threats
 - (c) Monitoring Challenges
- (2) Introduction to Security Onion
 - (a) Components
 - (b) Data types
- (3) Security Onion in the Cloud
 - (a) Facilitating cloud-based intrusion detection and monitoring with traffic mirroring
 - (b) Ingesting telemetry from external/vendor-specific sources
- (4) Automating the Onion
 - (a) Automating Security Onion Deployment

This talk assumes you have secured your individual AWS accounts at the basic level by locking down your root accounts with 2FA, and etc.

For more details on the workshop pre-requisites, please refer the following link:

<https://docs.google.com/document/d/1kYHM3B3Opok4UXZALBKdYsJppPhNbBMUovNR4dclnhg/edit?usp=sharing>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Performance

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Rogues Vlg

SpeakerBio:Daniel Roy

No BIO available

Description:

In this hybrid performance talk, Daniel will introduce you to the storied history of card cheats and con games and demonstrate some of the most legendary scams – and won't have to bet a penny!

Daniel Roy is a magician who specializes in the most difficult branch of card manipulation: the sleight of hand techniques used by professional card cheats. He has appeared at the World-Famous Magic Castle in Hollywood, and his audiences have included Hollywood actors, millionaires, and members of U.S. Congress. In 2019, he received the Milbourne Christopher award for Close-Up Magician of the Year.

Rogues Village activities will be streamed via Twitch.

Twitch: <https://www.twitch.tv/roguesvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Performance

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Rogues Vlg

SpeakerBio: Daniel Roy

No BIO available

Description:

In this hybrid performance talk, Daniel will introduce you to the storied history of card cheats and con games and demonstrate some of the most legendary scams – and won't have to bet a penny!

Daniel Roy is a magician who specializes in the most difficult branch of card manipulation: the sleight of hand techniques used by professional card cheats. He has appeared at the World-Famous Magic Castle in Hollywood, and his audiences have included Hollywood actors, millionaires, and members of U.S. Congress. In 2019, he received the Milbourne Christopher award for Close-Up Magician of the Year.

Rogues Village activities will be streamed via Twitch.

Twitch: <https://www.twitch.tv/roguesvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Phirautee

When: Saturday, Aug 8, 12:00 - 13:50 PDT

Where: See Description or Village

SpeakerBio: Viral Maniar

Viral Maniar is currently working as Technical Manager at RiskIQ managing the attack surface outside of the firewall for clients in the APAC region through his boutique cyber security firm Preemptive Cyber Security (www.preemptivecybersec.com) providing offensive and defensive consulting services based in Australia. Viral has provided security consulting services for over 8 years including infrastructure (internal-external), application penetration testing, vulnerability assessments, wireless penetration testing, social engineering, red team engagements, API testing, Thick & Thin client testing and cloud architecture security reviews to numerous clients across various industries in the APAC region. Viral has presented at conferences like Black Hat, ROOTCON and (ISC)2. Viral has also participated in a number of bug bounty programs and won awards for responsible disclosure of security vulnerabilities. In his leisure time, he enjoys developing security tools and maintains several projects on the GitHub. He has achieved industry certifications such as Offensive Security Certified Professional (OSCP) and SANS GPEN - Network Penetration Testing. Twitter: @ManiarViral / @PreemptiveCyber

Description:

Over the past few years, ransomware has gone wild and organisations around the world are getting targeted leading to the damage and disruption. As we all know that the threat landscape is changing rapidly and we hear the fuss about ransomware infection at the offices or read about it in the news.

Have you ever wondered how threat actors are writing ransoms? What level of sophistication and understanding is required to target an organisation? In this demo, we will utilise the native Windows commands to build ransomware and target a host via phishing.

Introducing Phirautee, a proof of concept crypto virus to spread user awareness about attacks and implications of ransoms. Phirautee is written purely using PowerShell and does not require any third-party libraries. This tool steals the information, holds an organisation's data to hostage for payments or permanently encrypts/deletes the organisation data. The tool uses public-key cryptography to encrypt the data on the disk.

Before encrypting, it exfiltrates the files from the network to the attacker. Once the files are encrypted and exfiltrated, the original files are permanently deleted from the host and then tool demands a ransom. The ransom is asked using the cryptocurrency for payments, so transactions are more difficult for law enforcement to trace.

During the demonstration of Phirautee, you will see a complete attack chain i.e. from receiving ransomware attack via a phishing email and how the files get encrypted on the compromised systems. A detailed walkthrough of the source code would be provided to understand how hackers utilise simple methods to create something dangerous. I will end the demo with several defence mechanisms by performing forensics analysis on Phirautee using publicly available tools.

Audience: Offense

Interact @ #dl-maniar-phirautee-text: <https://discord.com/channels/708208267699945503/730256398277148774>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://github.com/Viralmaniar/Phirautee>

Return to Index - Add to  - ics [Calendar](#) file

Title: Pickpocketing @ Home

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: Rogues Vlg

SpeakerBio:James Harrison

No BIO available

Description:

James Harrison returns to share his pickpocketing tips (a smash hit at Rogues Village at DEFCON 27 last year) via the internet. In this talk, James will show you how to practice your own pickpocketing skills inside your very own home! Come take a peek inside James' own setup, and learn some of his tricks of the trade. Safeguard yourself while learning a new skill!

Rogues Village activities will be streamed via Twitch.

Twitch: <https://www.twitch.tv/roguesvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Saturday - 11:00-11:59 PDT

Title: Playing with Electricity: Hacking into Distribution Companies

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: ICS Vlg

Speakers: Can Demirel, Serkan Temel

SpeakerBio: Can Demirel

No BIO available

SpeakerBio: Serkan Temel

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Porcupine: Rapid and robust tagging of physical objects using DNA with highly separable nanopore signatures

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: BioHacking Vlg

SpeakerBio: Katie Doroschak

Katie Doroschak is a PhD candidate in the MISL lab in the Allen School for Computer Science & Engineering at the University of Washington. She specializes in data science & machine learning for computational & synthetic biology.

Description:

Molecular tagging is an approach to labeling physical objects using DNA or other molecules that can be used in cases where methods like RFID tags and QR codes are not suitable. No molecular tagging method exists that is inexpensive, fast and reliable to decode, and usable outside a lab setting to create or read tags. To address this, we present Porcupine, an end-user molecular tagging system that features DNA-based tags readable within seconds using a portable nanopore device. Porcupine's digital bits are represented by the presence or absence of distinct, nanopore-orthogonal DNA strands, which we call molecular bits (molbits). We classify molbits directly from the raw nanopore signal, avoiding basecalling. To extend the tag's shelf life, decrease readout time, and make tags robust to environmental contamination, molbits are prepared for readout during tag assembly and can be stabilized by dehydration. The result is an extensible, real time, high accuracy tagging system that includes a novel approach to developing nanopore-orthogonal barcodes.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PAYV - Sunday - 10:00-10:59 PDT

Title: PoS Terminal Security Uncovered

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: Payment Vlg

SpeakerBio: Aleksei Stennikov

No BIO available

Description:

"Everyone uses different types of payment hardware in order to pay by card everyday. But how often do you think, how secure is it?

The speaker will talk about the payment terminals hardware internals and the approach to the security of common manufacturers, typical vulnerabilities, approaches to research and the consequences of research related to the payment security. This presentation uncovers some of results from our payment security projects."

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Friday - 15:45-16:45 PDT

Title: PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS

When: Friday, Aug 7, 15:45 - 16:45 PDT

Where: ICS Vlg

SpeakerBio: Ben Gardiner

Ben Gardiner is a Senior Cybersecurity Research Engineer contractor at the National Motor Freight Traffic Association, Inc. (NMFTA) specializing in hardware and low-level software security. Prior to joining the NMFTA team in 2019, Gardiner held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations. He is a DEF CON Hardware Hacking Village (DC HHV) volunteer. He is chair of the SAE TEVEES18A1 Cybersecurity Assurance Testing TF (drafting J3061-2), and a voting member of the SAE Vehicle Electronic Systems Security Committee.

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - [ics Calendar file](#)

Title: PowerLine Truck Hacking: 2TOOLS4PLC4TRUCKS

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Car Hacking Vlg 001

Speakers: Ben Gardiner, Chris Poore

SpeakerBio: Ben Gardiner

Ben Gardiner is a Senior Cybersecurity Research Engineer contractor at the National Motor Freight Traffic Association, Inc. (NMFTA) specializing in hardware and low-level software security. Prior to joining the NMFTA team in 2019, Gardiner held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations. He is a DEF CON Hardware Hacking Village (DC HHV) volunteer. He is chair of the SAE TEVEES18A1 Cybersecurity Assurance Testing TF (drafting J3061-2), and a voting member of the SAE Vehicle Electronic Systems Security Committee.

SpeakerBio: Chris Poore

Chris Poore is a Senior Computer Engineer at Assured Information Security in Rome, NY and a member of the Systems Analysis and Exploitation (SAE) group. He works to analyze, understand, characterize, and exploit cyber systems using adversarial techniques with a focus on RF-enabled devices. He has experience writing code for software-defined radios and GNU Radio to reverse-engineer RF communication protocols and perform sophisticated attacks. Mr. Poore has a degree in Social Engineering, is an active somnambulist, was King of the Pirates for three years, and frequently violates PornHub's terms of service.

Description:

Trailer ABS functionality has been a regulated requirement in the US & Canada for decades now. The 'PLC4TRUCKS' technology that realizes this requirement is ubiquitous on the road today and can also be found in buses, trains and some other unexpected places. We are releasing tools to read and write PLC4TRUCKS traffic. The first, gr-j2497 is a GNU Radio flowgraph with custom block and the second is an extension to the Truck Duck tool released at DEF CON 24. With these tools in hand, attendees can read PLC traffic without touching the bus -- or control their own trailer air brake controllers connected at home and we will show them how

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUej1Q&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Practical Advice on Threat Hunting Panel

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: Blue Team VIg - Talks Track 1

Speakers: Plug, Roberto Rodriguez, Tony M Lambert, Valentina Palacín, Samir, Ruth Barbacil, Anna McAbee, Paul Melson

SpeakerBio: Plug

No BIO available

Twitter: [@plugxor](#)

SpeakerBio: Roberto Rodriguez

Roberto Rodriguez is a threat researcher and security engineer at the Microsoft Threat Intelligence Center (MSTIC) R&D team.

He is also the author of several open source projects, such as the Threat Hunter Playbook, Mordor, OSSEM, HELK and others, to aid the community development of techniques and tooling for threat research. He is also the founder of a new community movement to empower others in the InfoSec community named Open Threat Research.

Blog at <https://medium.com/@Cyb3rWard0g>

Twitter: [@Cyb3rWard0g](#)

<https://medium.com/@Cyb3rWard0g>

SpeakerBio: Tony M Lambert

Tony is a professional geek who loves to jump into all things related to detection and digital forensics. After working in enterprise IT administration and detection engineering for several years, he now applies his DFIR skills to research malware, detect malicious activity, and recommend remediation paths. Tony is a natural teacher and regularly shares his findings and expertise through blogs, research reports, and presentations at conferences and events.

Twitter: [@ForensicITGuy](#)

SpeakerBio: Valentina Palacín

Valentina is a Threat Intelligence Senior Analyst, specializing in tracking Advanced Persistent Threats (APTs) worldwide and using the ATT&CK Framework to analyze their tools, tactics and techniques. She is a self-taught developer with a degree in Translation and Interpretation from the Universidad de Málaga (UMA), and a Cyber Security Diploma from the Universidad Tecnológica Nacional (UTN).

She recently published an article on how to get started with Threat Hunting using Atomic Red Team on the blog she shares with Ruth Barbacil: <https://medium.com/intelforge>

She is one of Ekoparty's BlueSpace coordinators and a member of a new community movement named Open Threat Research founded by Roberto Rodriguez.

Twitter: [@fierytermite](#)

SpeakerBio: Samir

Security Researcher at Elastic Security focusing on detection engineering and threats hunting

SpeakerBio: Ruth Barbacil

Ruth Barbacil is an Information Systems Engineer (UTN FRBA) and a Threat Intelligence & Analytics Specialist at Deloitte Argentina. She has carried out tasks of investigation and analysis of Malware, Tactics, Techniques and Procedures (TTPs) and advanced persistent threats activities in order to help customers to defend and mitigate them. She's interested in Intelligence,

Malware Analysis and Threat Hunting.

Twitter: [@33root](#)

SpeakerBio:Anna McAbee

No BIO available

SpeakerBio:Paul Melson

No BIO available

Description:No Description available

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Sunday - 01:00-01:59 PDT

Title: Practical PCFG Password Cracking (Rebroadcast)

When: Sunday, Aug 9, 01:00 - 01:59 PDT

Where: Password Vlg

SpeakerBio: Matt Weir

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Saturday - 14:00-14:59 PDT

Title: Practical PCFG Password Cracking

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Password Vlg

SpeakerBio: Matt Weir

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Practical VoIP/UC Hacking Using Mr.SIP: SIP-Based Audit & Attack Tool

When: Sunday, Aug 9, 15:30 - 15:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Ismail Melih Tas, Kubilay Ahmet Kucuk

SpeakerBio: Ismail Melih Tas, Senior Expert in Offensive Security (PhD), Private Bank

Melih Tas received B.Sc., M.Sc., and Ph.D. degrees in Computer Science & Engineering. He is working as Principal Penetration Tester in a private bank since 2015 in Istanbul, Turkey. He worked as multiple times award-winning entrepreneur and security expert in a private cybersecurity R&D company between 2010 and 2015 where he worked on funded projects. Previous to them, he also worked in a global troubleshooting center where he found the root causes of telecommunication security incidents and frauds and designed measures to prevent them from happening again. He wrote the National VoIP/UC Security Standard Draft by cooperating with Turkish Standards Institute. He is the author of open-source projects [Mr.SIP:SIP-Based Audit and Attack Tool](#) and [SIP-DD: SIP-Based DDoS Defense Tool](#). He holds an OSCP certificate. He is an active speaker in hacker conferences including Black Hat Arsenal, Offzone and Nopcon. He likes to do bug bounty hunting in his spare time. His research interests include the design and analysis of both offensive and defensive security mechanisms in the fields of VoIP Security, Network Security, and Web/Mobile Application Security.

Twitter: [@artinscience](#)

SpeakerBio: Kubilay Ahmet Kucuk, Senior Security Researcher (PhD), University of Oxford

Kubilay Ahmet Kucuk is a DPhil (Ph.D.) candidate at the University of Oxford. His research interests include the problem of secure remote computation, and architectures with TPM, TEEs, ARM TZ, seL4. With a focus on SGX, he received Ph.D. studentship from Intel and completed the AppTRE (Trustworthy Remote Entity) project in Prof. Andrew Martin's group. Before Oxford, he was a research assistant for five years at ETH Zürich, in D-MAVT Simulation Group. He led the software engineering in two CTI/Innosuisse funded projects in Industry 4.0 domain. These projects, the Face-gear Drive and the Next-Generation Virtual Feeder resulted in software products alive in the industry other than the journals.

Description:

In this talk, we will introduce the most comprehensive offensive VoIP security tool ever developed, Mr.SIP (comprehensive version). We will make a live attack demonstration using Mr.SIP in our security laboratory. Furthermore, we will also introduce novel SIP-based attacks using the vulnerabilities we found in the SIP retransmission mechanism and reflection logic.

Mr.SIP is developed to assist security experts and system administrators who want to perform security tests for VoIP systems and to measure and evaluate security risks. It quickly discovers all VoIP components and services in a network topology along with the vendor, brand, and version information, detects current vulnerabilities, configuration errors. It provides an environment to assist in performing advanced attacks to simulate abuse of detected vulnerabilities. It detects SIP components and existing users on the network, intervenes, filters and manipulates call information, develops DoS attacks, breaks user passwords, and can test the server system by sending irregular messages.

Status-controlled call flow and ability to bypass anomaly systems stand out as Mr.SIP's unique aspects. It also has strengths and competencies in terms of advanced fake IP address generation, fuzzing, password cracker, interactive inter-module attack kit, and MiTM features.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

[Return to Index](#) - Add to  - ics [Calendar](#) file



DEFCON DEFCON

DEFCON DEFCON



DEFCON DEFCON

DEFCON DEFCON



DEFCON DEFCON

DEFCON DEFCON



DEFCON DEFCON

DEFCON DEFCON

HRV - Saturday - 13:30-13:59 PDT

Title: Practice 'Net' via Discord

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: See Description or Village

Description:

In this 'demo', we'll be hosting a practice 'net' (ham-speak for on-air meeting) on the #ham-get-on-the-air-voice channel in the village. All persons, even non-hams, are invited to join us in this practice so you can become familiar with expected etiquette. And later on, you can put these skills to use on the DMR Net!

This event will be held exclusively on Discord, in the #ham-get-on-the-air-voice channel.

Discord: <https://discord.com/channels/708208267699945503/736674175179292673>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Product Cybersecurity: Secure Airplane Development Lifecycle

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: Aerospace VIg

SpeakerBio:Michael Vanguardia

Michael Vanguardia is an Associate Technical Fellow and Senior Product Cybersecurity Engineer for Boeing Commercial Airplanes, out of Seattle, Washington. In this role he supports security throughout the entire airplane development cycle; from security architecture definition and design, through software development and verification. This includes the execution of security testing against embedded avionic systems and networks across Boeing's fleet of commercial aircraft. Recently, Michael's role has been extended to spearhead security researcher engagement and airplane cyber incident investigations. Michael comes with 20+ years of experience working with space systems and avionics across the Department of Defense and the Commercial Aviation sectors.

Description:

The Aviation industry has always focused on safety and with the advent of the e-enabled aircraft must now also contend with cybersecurity threats. Malicious intent via cyber means is a new area of concern that needs to be accounted for during airplane design, development, and verification. This talk will provide an overview of Boeing's Secure Airplane Development Lifecycle and activities that the Commercial Airplane, Product Security organization has undertaken to enhance the cyber resiliency of commercial aircraft.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Friday - 12:00-12:30 PDT

Title: Proposed Mitigation Measures to Address a Disruption Such as The Economic Impact of COVID -19 on Transaction Capacity and Fees in Monero

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: Monero Vlg

SpeakerBio:Dr. Francisco "ArticMine" Cabañas
No BIO available

Description:

Monero uses an adaptive block weight based upon the CryptoNote excess size penalty with a median over the last 100 blocks, cryptonote.org/whitepaper.pdf, to provide the capacity for increases and decreases in the number of transactions. In 2019 this adaptive block weight was modified by the introduction of a long term median over the last 100,000 blocks to mitigate against a sharp increase in the block weight, due to possible spam attacks. We will consider the scenario of external economic events causing a sharp decrease in the number of transactions after several years of growth, followed by a recovery and then further growth several months later. We will also consider the possibility of a sharp increase in the number of transactions, due to economic disruptions, during the current COVID-19 pandemic. and in its aftermath. We will propose changes to the Monero adaptive block weight in order to mitigate against a sharp increase in transaction fees and allow for a smooth recovery, and further growth in the block weight after a sharp drop in the number of transactions . The period between the initial drop in the number of transactions to the full recovery with further growth of the block weight would be in the order of months.

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

Return to Index - Add to  - ics [Calendar](#) file

VMV - Saturday - 16:00-16:30 PDT

Title: Protecting Elections with Data Science -- A Tool for 2020 and Beyond

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: Voting Vlg

SpeakerBio: Stephanie Singer , Consultant and Data Scientist, Verified Voting

No BIO available

Description:

What are the possibilities, and challenges, for using data science to protect elections? Stephanie Singer will describe an open source tool to aid in quick consolidation of election results, and a public-facing web front end planned for November 2020 and beyond.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Purple On My Mind: Cost Effective Automated Adversary Simulation (Intermediate)

When: Friday, Aug 7, 19:30 - 20:30 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio: Mauricio Velazco

Mauricio Velazco (@mvelazco) is a Peruvian, Infosec professional who started his career as a penetration tester and jumped to the blue team 8 years ago. He currently leads the Threat Management team at a Fortune 500 where he focuses on threat detection/hunting and adversary simulation. Mauricio has presented and hosted workshops at conferences like Defcon, Derbycon, BSides and the SANS Threat Hunting Summit. He holds a few certifications including OSCP and OSCE.

Twitter: [@mvelazco](https://twitter.com/mvelazco)

Description:

Automated adversary simulation is often perceived as a hard, dangerous and complicated program to implement and run. Fear no longer, our methodology and tooling will let you test and measure your defenses throughout your production environment to test not only your detection rule's resilience but the whole event pipeline as well as your team's response procedures. In this talk, we'll share with the audience the open source tools we built and the methodology we use that will allow them to hit the ground running at nearly no cost.

Introduction (5 min)

Automated Adversary simulation - Design & Methodology (10 min)

State of the art (3 min)

Our approach (25 min)

Takeaways (3 min)

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: PWN The World

When: Sunday, Aug 9, 07:15 - 08:15 PDT

Where: Red Team VIg

SpeakerBio:Chris Kubecka

Chris Kubecka - "Fearless and powerful speaker, saves countries, fights cyber terrorism, advises several governments as a subject matter expert on cyber warfare national defense. Profiled by major media in the USA and Europe. USAF military combat veteran, former military aviator, and USAF Space Command. Defends critical infrastructure and handles country level cyber incidents, cyberwarfare, and cyber espionage. Reconnected Saudi Aramco international business operations & established digital security after the world's most devastating cyberwarfare attack. Developing the highest level of exploit code against IT/IOT/ICS SCADA control systems whilst working with governments. Involved in the world's biggest hacks, advising nations, NATO, Europol, Interpol exposing corruption and national security risks.

"She is a go-to professional for governments. There are only a certain number who can both frame the problem conceptually and put it in straight fuc**** English so somebody can understand. And she can do that.

Description:

Want to learn the basics of how to hack cool industrial IOT, industrial control systems and technology that moves the world? How to find them, leverage weaknesses in protocols & systems. Turn engineer technical tools into dual use reconnaissance and attack tools. Components of energy grids, digital security systems, production systems and more.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Pwn2Own Qualcomm compute DSP for fun and profit

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Slava Makkaveev , Security Researcher, Check Point

Slava Makkaveev is a Security Researcher at Check Point. Holds a PhD in Computer Science. Slava has found himself in the security field more than ten years ago and since that gained vast experience in reverse engineering and vulnerability research. Recently Slava has taken a particularly strong interest in mobile platforms and firmware security.

Description:

Qualcomm Snapdragon SoC integrates multiple subsystems, each one is customized for a particular application domain. Compute digital-signal processor (cDSP) is a subsystem which allows a mobile device to process simple sets of data with high performance on low power. In the talk we will show that this little studied proprietary subsystem has many security problems that open the door to malicious Android applications for PE and DoS attacks of the device.

For security reasons, the cDSP is licensed for programming by OEMs and by a limited number of third-party software vendors. The code running on DSP is signed by Qualcomm. However, we will demonstrate how an Android application can bypass Qualcomm's signature and execute privileged code on DSP, and what further security issues this can lead to.

Hexagon SDK is the official way for the vendors to prepare DSP related code. We discovered serious bugs in the SDK that have led to the hundreds of hidden vulnerabilities in the Qualcomm-owned and vendors' code. The truth is that almost all DSP executable libraries embedded in Qualcomm-based smartphones are vulnerable to attacks due to issues in the Hexagon SDK. We are going to highlight the auto generated security holes in the DSP software and then exploit them.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord (#track-1-live).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

Return to Index - Add to  - ics [Calendar](#) file

Title: Pwning Your Resume

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Career Hacking Vlg

SpeakerBio: Kris Rides

No BIO available

Description:

Does your resume writing professional know the Cyber Security Industry? If not why are you paying them to do a job you're better qualified to do your self? Put that money towards building your knowledge or something that will really help further your career. This presentation will focus on what makes an excellent cyber security resume and how to write it yourself.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: PyRDP: Remote Desktop Protocol Monster-in-the-Middle (MITM) and Library

When: Friday, Aug 7, 12:00 - 13:50 PDT

Where: See Description or Village

SpeakerBio: Olivier Bilodeau

Olivier Bilodeau is leading the Cybersecurity Research team at GoSecure. With more than 10 years of infosec experience, he enjoys luring malware operators into his traps, writing tools for malware research, reverse-engineering all-the-things and vulnerability research. Passionate communicator, Olivier has spoken at several conferences like BlackHat, Defcon, Botconf, SecTor, Derbycon, HackFest and more. Invested in his community, he co-organizes MontréalHack, a monthly workshop focused on hands-on CTF problem solving, and NorthSec, a large non-profit conference and CTF based in Montreal.

Description:

PyRDP is a Remote Desktop Protocol (RDP) monster-in-the-middle (MITM) tool and library useful in intrusion testing and malware research. Its out of the box offensive capabilities can be divided in three broad categories: client-side, MITM-side and server-side. On the client-side PyRDP can actively steal any clipboard activity, crawl mapped drives and collect all keystrokes. On the MITM-side PyRDP records everything on the wire in several formats (logs, json events), allows the attacker to take control of an active session and performs a pixel perfect recording of the RDP screen. On the server-side, on-logon PowerShell or cmd injection can be performed when a legitimate client connects. Over the last year, we implemented several features that we are going to uncover in this brand-new demo lab workshop: a headless mode that allows deployment on systems with less resources or without an X11 stack, a fully transparent layer-2 deployment capability leveraging IP_TRANSPARENT sockets, a brand new Windows Graphical Device Interface (GDI) implementation and the ability to convert recorded sessions into MP4 videos. On the malware research side, PyRDP can be used as part of a fully interactive honeypot. It can be placed in front of a Windows RDP server to intercept malicious sessions. It can replace the credentials provided in the connection sequence with working credentials to accelerate compromise and malicious behavior collection. It also saves a visual and textual recording of each RDP session, which is useful for investigation or to generate IOCs. Additionally, PyRDP saves a copy of the files that are transferred via the drive redirection feature, allowing it to collect malicious payloads.

Audience: Offense and Malware Researchers

Interact @ #dl-bilodeau-pyrdp-text: <https://discord.com/channels/708208267699945503/730256435916832849>

Watch @ #dl-video2-voice: <https://discord.com/channels/708208267699945503/734027778646867988>

Github: <https://github.com/GoSecure/pyrdp>

Forum: <https://forum.defcon.org/node/233124>

Return to Index - Add to  - ics [Calendar](#) file

Title: PyRDP: Remote Desktop Protocol Monster-in-the-Middle (MITM) and Library

When: Saturday, Aug 8, 14:00 - 15:50 PDT

Where: See Description or Village

Speakers: Olivier Bilodeau, Alexandre Beaulieu

SpeakerBio: Olivier Bilodeau

Olivier Bilodeau is leading the Cybersecurity Research team at GoSecure. With more than 10 years of infosec experience, he enjoys luring malware operators into his traps, writing tools for malware research, reverse-engineering all-the-things and vulnerability research. Passionate communicator, Olivier has spoken at several conferences like BlackHat, Defcon, Botconf, SecTor, Derbycon, HackFest and more. Invested in his community, he co-organizes MontréalHack, a monthly workshop focused on hands-on CTF problem solving, and NorthSec, a large non-profit conference and CTF based in Montreal.

SpeakerBio: Alexandre Beaulieu

Alexandre is a security researcher working for GoSecure. His area of expertise is reverse engineering, binary exploitation and tool development. His previous experience as a software developer covers a broad spectrum of topics ranging from low-level systems and binary protocols to web applications. Prior to joining the research team, Alexandre spent time as an Ethical Hacker honing his offensive security skills. His areas of interest include binary analysis, compiler theory and systems programming. Alexandre gives back to the Montréal infosec community by volunteering his time, contributing workshops and designing application security challenges for events like MontréalHack and REcon.

Description:

PyRDP is a Remote Desktop Protocol (RDP) monster-in-the-middle (MITM) tool and library useful in intrusion testing and malware research. Its out of the box offensive capabilities can be divided in three broad categories: client-side, MITM-side and server-side. On the client-side PyRDP can actively steal any clipboard activity, crawl mapped drives and collect all keystrokes. On the MITM-side PyRDP records everything on the wire in several formats (logs, json events), allows the attacker to take control of an active session and performs a pixel perfect recording of the RDP screen. On the server-side, on-logon PowerShell or cmd injection can be performed when a legitimate client connects. Over the last year, we implemented several features that we are going to uncover in this brand-new demo lab workshop: a headless mode that allows deployment on systems with less resources or without an X11 stack, a fully transparent layer-2 deployment capability leveraging IP_TRANSPARENT sockets, a brand new Windows Graphical Device Interface (GDI) implementation and the ability to convert recorded sessions into MP4 videos. On the malware research side, PyRDP can be used as part of a fully interactive honeypot. It can be placed in front of a Windows RDP server to intercept malicious sessions. It can replace the credentials provided in the connection sequence with working credentials to accelerate compromise and malicious behavior collection. It also saves a visual and textual recording of each RDP session, which is useful for investigation or to generate IOCs. Additionally, PyRDP saves a copy of the files that are transferred via the drive redirection feature, allowing it to collect malicious payloads.

Audience: Offense and Malware Researchers

Interact @ #dl-bilodeau-pyrdp-text: <https://discord.com/channels/708208267699945503/730256435916832849>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Github: <https://github.com/GoSecure/pyrdp>

Forum: <https://forum.defcon.org/node/233124>

Return to Index - Add to  - ics [Calendar](#) file

Title: Quantum Computers & Cryptography

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio:I. Shaheem

Imran Shaheem joined Cyberis Limited in early 2018 following the successful completion of an MSc in Theoretical Physics (Gravity, Particles and Fields) at the University of Nottingham. Prior to joining Cyberis, Imran participated in online bug bounty programs which led to private security research work for a Fortune 10 company. In conjunction to this, his work earned him BugCrowd's VIP researcher accolade in 2017, placing him in the top 300 of over 50,000 researchers who use the platform.

Description:

Quantum Cryptography has exploded, both in terms of active research and public awareness, since scientific interest in the field took off in the 90s. The ramifications of quantum computers on classical (current) cryptography and what will be considered the standard for secure communication in the near future mandates a radical change in our approach. Successful trials that secure communication through the unique properties of quantum physics have already been undertaken. Progress in quantum technologies has been swift in the last decade. Quantum Key Distribution (QKD) systems have been tested by banks and governments, similar systems were deployed at the 2010 World Cup in South Africa. In 2017, researchers held a QKD-protected video conference between China and Austria using the quantum satellite Micius as a trusted relay, further strides and greater worldwide adoption is anticipated for the coming decade. This presentation will start with an overview of quantum information and its impact on classical cryptography. Following this, we'll delve into the weird and wonderful world of quantum physics and its relationship to cryptography; the making, breaking and subsequent fixing of quantum protocols. We'll discuss how much of the theoretical possibilities that are achievable with quantum computers we'll likely see in practice in the near future and how we can go about building our own relatively inexpensive quantum lab to test new protocols and quantum devices. Everything will be discussed from an InfoSec perspective, looking at how testing methodologies can be adapted and what remediation advice can be given to clients during the transitory period as we migrate to quantum safe solutions. While some light mathematics may be called upon during the presentation, this talk is aimed squarely at cyber security professionals and enthusiasts, not physicists or mathematicians.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

Return to Index - Add to  - ics [Calendar](#) file

Title: Quark Engine - An Obfuscation-Neglect Android Malware Scoring System (Beginner)

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: Blue Team VIg - Talks Track 1

Speakers: JunWei Song, KunYu Chen

SpeakerBio: JunWei Song

JunWei is a Security Researcher from Taiwan. A paranoid Pythonista who focuses on cybersecurity, reverse engineering, and malware analysis. And as a CPython contributor, PyCon Taiwan Program Committee, presented at DEFCON, HITB, EuroPython, PyCon Taiwan, PyCon Korea, PyCon Malaysia. He's the co-founder of Quark-Engine and a security research group, TWBGC.

Twitter: [@JunWei_Song](https://twitter.com/JunWei_Song)

SpeakerBio: KunYu Chen

No BIO available

Description:

Android malware analysis engine is not a new story. Every antivirus company has their own secrets to build it. With python and curiosity, we develop a malware scoring system from the perspective of Taiwan Criminal Law in an easy but solid way.

We have an order theory of criminal which explains stages of committing a crime. For example, crime of murder consists of five stages, they are determined, conspiracy, preparation, start and practice. The latter the stage the more we're sure that the crime is practiced.

According to the above principle, we developed our order theory of android malware. We develop five stages to see if the malicious activity is being practiced. They are:

Permission requested.

Native API call.

Certain combination of native API.

Calling sequence of native API.

APIs that handle the same register.

We not only define malicious activities and their stages but also develop weights and thresholds for calculating the threat level of a malware.

Malware evolved with new techniques to gain difficulties for reverse engineering. Obfuscation is one of the most commonly used techniques. In this talk, we present a Dalvik bytecode loader with the order theory of android malware to neglect certain cases of obfuscation.

Inspired by the design principles of the CPython interpreter, our Dalvik bytecode loader consists of functionalities such as 1. Finding cross-reference and calling sequence of the native API. 2. Tracing the bytecode register. The combination of these functionalities (yes, the order theory) not only can neglect obfuscation but also match perfectly to the design of our malware scoring system.

Further, we will also show a case study of Android malware and demonstrate how the obfuscation technique is useless to our engine. Last but not least, we will be open-sourcing everything (Malware Scoring System, Dalvik Bytecode Loader) during our presentation.

Github: <https://github.com/quark-engine/quark-engine>

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ransom in the Cloud

When: Friday, Aug 7, 12:05 - 12:50 PDT

Where: Cloud Vlg

SpeakerBio: Spencer Gietzen

Spencer Gietzen comes from a background in web development and penetration testing. He is now a Cloud Security Researcher at CrowdStrike, spearheading research and development of new and upcoming cloud threats. Spencer has published a variety of research blogs and developed cloud security tools for the open source community, such as Pacu, an offensive AWS pentesting framework.

Twitter: [@SpenGietz](#)

Description:

Traditional ransomware has become a popular tool for cybercriminals to make their buck and has cost a variety of industries hundreds of millions to billions of dollars in recent years. As trends change and corporations move from traditional data centers to cloud environments like AWS, GCP, and Azure, adversaries are adapting their techniques to match the new climate. Because of this, attackers abusing cloud APIs rather than host/network-based commands are becoming more prevalent. This talk explores the services most likely to be targeted by ransomware in AWS cloud, techniques that attackers may use, and preventative/detective measures to assist the blue team.

Spencer Gietzen comes from a background in web development and penetration testing. He is now a Cloud Security Researcher at CrowdStrike, spearheading research and development of new and upcoming cloud threats. Spencer has published a variety of research blogs and developed cloud security tools for the open source community, such as Pacu, an offensive AWS pentesting framework.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Realistic Trends in Vulnerability based on Hacking into Vehicle

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Car Hacking VIg 001

Speakers:Ryosuke Uematsu,Shogo Nakao,Ryoichi Teramura,Tatsuya Katsuhara

SpeakerBio:Ryosuke Uematsu

No BIO available

SpeakerBio:Shogo Nakao

No BIO available

SpeakerBio:Ryoichi Teramura

No BIO available

SpeakerBio:Tatsuya Katsuhara

No BIO available

Description:

This presentation introduces the trends in the ECU vulnerabilities and the mitigations against the ones, and also our assessment method.

We have worked with more than 10 auto manufacturers and suppliers, and we have assessed a lot of their ECUs in development. Here, we had already found over 200 vulnerabilities, making it reveal the trends in both the vulnerabilities and mitigations statistically. Some of them make a huge impact on automotive safety, that is we can hack into the vehicle via the wireless connection.

#chv-track001-text: <https://discord.com/channels/708208267699945503/735650705930453173>

YouTube: <https://www.youtube.com/watch?v=VvojAHUej1Q&feature=youtu.be>

Twitch: <https://www.twitch.tv/chvtrack001>

Return to Index - Add to  - ics [Calendar](#) file

Title: Red Team Village Announcements and Remarks

When: Thursday, Aug 6, 07:30 - 07:59 PDT

Where: Red Team Vlg

Speakers:Joseph Mlodzianowski (cedoXx),Omar r

SpeakerBio:Joseph Mlodzianowski (cedoXx)

No BIO available

Twitter: [@cedoXx](#)

SpeakerBio:Omar r

No BIO available

Description:No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Red Team Village Closing Ceremony and Announcement of Winners of CTF and CyberWraith

When: Sunday, Aug 9, 16:00 - 16:59 PDT

Where: Red Team Vlg

Speakers:Joseph Mlodzianowski (cedoXx),Omar r

SpeakerBio:Joseph Mlodzianowski (cedoXx)

No BIO available

Twitter: [@cedoXx](#)

SpeakerBio:Omar r

No BIO available

Description:No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

RTV - Friday - 09:30-15:59 PDT

Title: Red Team Village CTF - Finals

When: Friday, Aug 7, 09:30 - 15:59 PDT

Where: Red Team Vlg

Description:

The first part of the CTF will be qualifiers in jeopardy format, then the top teams will move into finals where each will compete in the Pendulum Red Team environment, a full corporate network (each team will have their own env) .

Skills required to win: pentesting/red team, scripting, reversing, exploitation, privilege escalation, pivoting, exploit development and anti-virus evasion.

Info: <https://redteamvillage.io/ctf.html>

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar](#) file

RTV - Thursday - 09:00-08:59 PDT

Title: Red Team Village CTF - Prequal

When: Thursday, Aug 6, 09:00 - 08:59 PDT

Where: Red Team Vlg

Description:

The first part of the CTF will be qualifiers in jeopardy format, then the top teams will move into finals where each will compete in the Pendulum Red Team environment, a full corporate network (each team will have their own env) .

Skills required to win: pentesting/red team, scripting, reversing, exploitation, privilege escalation, pivoting, exploit development and anti-virus evasion.

Info: <https://redteamvillage.io/ctf.html>

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar](#) file

RTV - Friday - 07:30-07:59 PDT

Title: Red Team Village Opening Remarks

When: Friday, Aug 7, 07:30 - 07:59 PDT

Where: Red Team Vlg

Speakers: Joseph Mlodzianowski (cedoXx), Omar r

SpeakerBio: Joseph Mlodzianowski (cedoXx)

No BIO available

Twitter: [@cedoXx](#)

SpeakerBio: Omar r

No BIO available

Description: No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Red Teaming: Born from the Hacker Community

When: Friday, Aug 7, 09:15 - 10:15 PDT

Where: Red Team VIg

SpeakerBio:Chris Wysopal

Chris Wysopal is currently Veracode's CTO and Co-Founder. He is responsible for the company's software security analysis capabilities. One of the original vulnerability researchers and a member of L0pht Heavy Industries, Chris has testified on Capitol Hill in the US on the subjects of government computer security and how vulnerabilities are discovered in software. He published his first advisory in 1996 on parameter tampering in Lotus Domino and has been trying to help people not repeat this type of mistake for 15 years. Back in 1997 he first got paid for hacking someone else's network and later a company's web application. Chris was hooked and has been performing security testing one way or another since.

Description:No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Redefining patient safety in the digital era

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: BioHacking Vlg

Speakers: Dena Medelsohn, Jen Goldsack

SpeakerBio: Dena Medelsohn

Dena Medelsohn is a passionate consumer advocate and boldly believe in data rights and access to quality healthcare. Dena is the director of health policy and data governance at Elektra Labs. Previously, Dena was the senior attorney at Consumer Reports.

SpeakerBio: Jen Goldsack

Jen Goldsack is the executive director of the Digital Medicine Society (DiMe), a 501c3 dedicated to advancing digital medicine to optimize human health. Jen's research focuses on applied approaches to the safe, effective & equitable use of digital technologies to improve health, healthcare & health research.

Description:

Digital technologies are the future of medicine--and perhaps also public health--but these innovative tools that offer great promise for higher quality, more affordable, more accessible care also pose new risks to patients.

Using real-world examples, this presentation will make the case for expanding the list of harms considered when determining the risk-benefit profile of a medical product in the digital era of health. We will consider security practices -- and sometimes their absence -- and disparities in both access to technologies and technical literacy.

Digital technologies - and in particular remote monitoring technologies such as wearables and other in - home smart sensors have the potential to transform health, healthcare, and health research. But these innovative tools also pose new risks to patients.

Risk-benefit analysis is the bedrock of clinical decision making, from formulating individual treatment plans to drug approval decisions. However, while shaky data rights in the United States put patients at risk when they use digital health products, these risks are poorly understood and rarely included in risk-benefit analyses.

This presentation will illustrate the new risks to patients posed by their digital health footprint--from challenges accessing health care to discrimination in the workplace--and explain for readers why data rights and security must be folded into a contemporary definition of 'patient safety'.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: redlure

When: Sunday, Aug 9, 10:00 - 11:50 PDT

Where: See Description or Village

SpeakerBio:Matthew Creel

Matt has been a member of the Schneider Downs cybersecurity practice since 2017 where he helps provide clients with penetration testing, red teaming and incident response services. One of Matt's focuses is offensive tool development, notably password spraying and phishing tools. Matt has served clients in manufacturing, healthcare, automotive, financial and higher education industries.

Description:

redlure can be described as a distributed phishing platform. There is a centralized API (redlure-console) where you can create the different aspects of your phishing campaigns. This console controls secondary servers running a more basic API (redlure-workers) that do the actual hosting of your phishing sites/files and communicate results back to the main server. Obviously there are existing tools that can accomplish phishing, but here are a few features to this tool that differentiate it and will be described in the abstract.

Audience: Offense

Interact @ #dl-creel-redlure-text: <https://discord.com/channels/708208267699945503/730256326868860949>

Watch @ #dl-video2-voice: <https://discord.com/channels/708208267699945503/734027778646867988>

Forum: <https://forum.defcon.org/node/233131>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: redlure

When: Friday, Aug 7, 16:00 - 17:55 PDT

Where: See Description or Village

SpeakerBio: Matthew Creel

Matt has been a member of the Schneider Downs cybersecurity practice since 2017 where he helps provide clients with penetration testing, red teaming and incident response services. One of Matt's focuses is offensive tool development, notably password spraying and phishing tools. Matt has served clients in manufacturing, healthcare, automotive, financial and higher education industries.

Description:

redlure can be described as a distributed phishing platform. There is a centralized API (redlure-console) where you can create the different aspects of your phishing campaigns. This console controls secondary servers running a more basic API (redlure-workers) that do the actual hosting of your phishing sites/files and communicate results back to the main server. Obviously there are existing tools that can accomplish phishing, but here are a few features to this tool that differentiate it and will be described in the abstract.

Audience: Offense

Interact @ #dl-creel-redlure-text: <https://discord.com/channels/708208267699945503/730256326868860949>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Forum: <https://forum.defcon.org/node/233131>

Return to Index - Add to  - ics [Calendar](#) file

Title: RedTeamOps - Managing Red Team Infrastructure as a Red Teamer

When: Sunday, Aug 9, 03:30 - 04:30 PDT

Where: Red Team Vlg

SpeakerBio: Mert Can Coşkuner

Mert Can Coşkuner is a Security Engineer at Trendyol. He is maintaining a Penetration Testing and Malware Analysis blog at medium.com/@mcoskuner. In his free time Mert Can is performing mobile malware research and threat intelligence.

Description:

Red team operations involve many skills, the operation requires a lot of monitoring, consolidating and caution. In order to perform red team operations faster, and stealthier without thinking about the infrastructure every team has its' own habits and standarts. However, there is a problem with those habits and standarts; - There are tons of tools but no operation management, - No aggregation between these tools, - When OPSEC fails due to problems above or any other reason, it's essential to possess the capability of maintaining robust infrastructure which can be recreated if discovered, and more importantly, without any issues upon deployment. In this talk, infrastructure challenges we face as a red teamer will be discussed. Along with challenges, a solution will be proposed based on DevOps practices such as; - Design your infrastructure based on the standarts and habits which your team has - Create playbooks which suits your needs based on your design - Create CI pipeline to test and maintain your playbooks

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Remediation Framework - Auto respond to AWS nightmares.

When: Sunday, Aug 9, 11:45 - 12:30 PDT

Where: Cloud Vlg

Speakers: Sahir Khan, Justin Paglierani

SpeakerBio: Sahir Khan

Sahir Khan is Senior Security Engineer at Flatiron Health focused on Cloud Security and has deep interests in Security automation.

SpeakerBio: Justin Paglierani

Justin Paglierani is a Staff Security Engineer at Flatiron Health. Prior to Flatiron, Justin worked at Bishop Fox and within the Federal Reserve System.

Description:

Remediation Framework is event driven, near real time, multi account, serverless platform which identifies and remediates AWS security issues to ensure AWS usage is in compliance with a set of rules. Major focus is on remediations for misconfigurations which could make resources(ec2-ami,snapshots, s3, redshift, rds..) publicly exposed, making it low lift for attackers to get foothold or data exfiltration. The framework is easily customizable, giving the ability to add new modules for AWS resources you want to watch for/automatically fix, when they become non compliant.

This talk will be structured as below:

Introductions (1-2 minutes): Brief bio of what we do. Background (3 minutes): Introduction to the problem statement which led us to work on automated remediation. First iteration - Independent Lambda for remediation of each resource and the challenges we faced. Introduction to the Framework: (5 minutes) A walkthrough of the framework, how it is pieced together to support event driven remediation for multiple AWS accounts and regions. Demo and Q&A (10 minutes): We will open source and demo the Remediation Framework by making few AWS resources publicly exposed and letting the remediation framework fix it automatically.

YouTube: <https://www.youtube.com/watch?v=DSipgVIsAfo>

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

Return to Index - Add to  - ics [Calendar](#) file

VMV - Saturday - 12:30-12:59 PDT

Title: Remote Online Balloting Delivery and Marking Options and Security Considerations for Absentee Voting During the COVID-19 Pandemic

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: Voting VIg

Speakers: Susan Greenhalgh, Steve Newell

SpeakerBio: Susan Greenhalgh , Senior Advisor on Election Security, Free Speech for People
No BIO available

SpeakerBio: Steve Newell , Project Director, Center for Scientific Evidence in Public Issues, American Association for the Advancement of Science, Center for Scientific Evidence in Public Issues
No BIO available

Description:

As States grapple with the difficult task of holding elections during the novel coronavirus pandemic, election administrators are exploring and implementing technology to deliver blank ballots electronically. The expansion of vote by mail in many states also necessitates a remote accessible ballot marking option for voters with disabilities.

A number of available systems allow the voter to receive a blank ballot electronically, mark it on their computer and print it for mailing or drop off without transmitting the voted ballot to the election office. However, these remote accessible ballot marking systems can be designed in different ways that have significantly different security and privacy profiles.

We explore the different architectures for remote ballot marking, comparing systems that conduct the marking process over the internet, (on a remote server), and those that mark ballots statelessly, on the client's device. We consider the security and privacy issues associated with both technologies, and offer specific recommendations to limit security and privacy risks.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

Return to Index - Add to  - ics [Calendar](#) file

PWDV - Friday - 22:00-22:30 PDT

Title: Result of Longer Passwords in Real World Application (Rebroadcast)

When: Friday, Aug 7, 22:00 - 22:30 PDT

Where: Password Vlg

SpeakerBio:Minga

No BIO available

Description:No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Friday - 15:00-15:30 PDT

Title: Result of Longer Passwords in Real World Application

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: Password Vlg

SpeakerBio:Minga

No BIO available

Description:No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Reverse Engineering the Tesla Battery Management System for Moar Powerrr!

When: Saturday, Aug 8, 16:30 - 16:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Patrick Kiley , Principal Security Consultant, Rapid7

Patrick Kiley (GXPN, GPEN, GAWN, GCIH, CISSP, MCSE) has over 18 years of information security experience working with both private sector employers and the Department of Energy/National Nuclear Security Administration (NNSA). While he was with the NNSA he built the NNSA's SOC and spent several years working for emergency teams. Patrick has performed research in Avionics security and Internet connected transportation platforms. Patrick has experience in all aspects of penetration testing, security engineering, hardware hacking, IoT, Autonomous Vehicles and CAN bus.

Twitter: [@gigstorm](https://twitter.com/gigstorm)

Description:

Tesla released the P85D in 2014. At that time the vehicle came with "insane mode" acceleration with a 0-60 time of 3.2 seconds. Later in July of 2015, Tesla announced "Ludicrous mode" that cut the 0-60 time down to 2.8 seconds. This upgrade was offered both new and as a hardware and firmware change to the existing fleet of P85D vehicles. Since then, Tesla has released newer ludicrous vehicles. What makes the P85D upgrade unique was how the process required changes to the vehicle's Battery Management System(BMS). The 'BMS' handles power requests from the drive units of the car. I was able to reverse engineer this upgrade process by examining the CAN bus messages, CAN bus UDS routines and various firmware files that I extracted from a car. I also decrypted and decompiled Python source code used for diagnostics to determine that the process involved replacing the contactors and fuse with higher current versions as well as modifying the current sensing high voltage "shunt" inside the battery pack. I then performed this process on an actual donor P85D. I bricked the car in the process, forcing me to pay to have it towed to another state so I could troubleshoot. I came to understand that the BMS is the deciding module that allows the drive units to have only as much power as the BMS allows. The car is fixed and is faster.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](https://discord.com/channels/708208267699945503/733079621402099732)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Reversing with Dynamic Data Resolver (DDR) – Best practice (Advanced)

When: Saturday, Aug 8, 09:00 - 09:59 PDT

Where: Blue Team Vlg - Talks Track 1

SpeakerBio: Holger Unterbrink

Holger is a security researcher working for Cisco Talos. His day job is to find and analyze new malware campaigns. He is the author of DDR and several other tools.

Twitter: [@hunterbr72](https://twitter.com/hunterbr72)

Description:

DDR is an IDA plugin that instruments binaries using the DynamoRIO framework. In this presentation we will show you best practices how to reverse engineer malware with DDR. The talk will discuss the internals of DDR and show you by demonstration, the advantages of the tool.

The DDR plugin can easily resolve the majority of dynamic values for registers and memory locations which are usually missed in a static analysis. It can help to find jump locations such as “call eax” or interesting strings such as “PE” which are decoded at runtime. The tool can be used to dump interesting buffers, and gives the opportunity to patch the binary at runtime to bypass anti-analysis techniques.

In this presentation we will show you best practices for working with this tool, and the many ways in which it can facilitate malware analysis. More details and features can be found here:

<https://blog.talosintelligence.com/2020/05/dynamic-data-resolver-1-0.html>

Blue Team Village activities in 'Talks Track 1' will be streamed to Twitch.

Twitch: <https://twitch.tv/BlueTeamVillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Reviewing MS08-067, Illustration Of An Old Chapter

When: Sunday, Aug 9, 02:15 - 03:15 PDT

Where: Red Team Vlg

SpeakerBio:Etizaz Mohsin

Etizaz Mohsin is an information security researcher and enthusiast. His core interest lies in low level software exploitation both in user and kernel mode, vulnerability research, reverse engineering. He holds a Bachelors in Software Engineering and started his career in Penetration Testing. He is an active speaker at international security conferences. He has achieved industry certifications, the prominent of which are OSCP, OSCE, OSWP, OSWE, OSEE, CREST CRT, CPSA, EWPTX, CEH.

Description:No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Rights You Can't Exercise Can't Protect You: Privacy by Design, Dark Patterns, and Cultural Context

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: Crypto & Privacy Vlg

Speakers: Ben Brook, Maritza Johnson, Megan DeBlois, Zach Singleton

SpeakerBio: Ben Brook

Ben Brook is the CEO and co-founder of Transcend, working to make it easy for companies to give users control over their data. Originally from Toronto, Canada, Brook is also a passionate and award-winning filmmaker.

SpeakerBio: Maritza Johnson

Maritza Johnson is Senior User Experience Researcher at Google Research. Her research interests include human-centered security and privacy with a focus on how end-users think about personal data management. Previously, she was a research at the independent nonprofit International Computer Science Institute.

SpeakerBio: Megan DeBlois

Megan DeBlois is a grad student at Oxford University, security consultant, and an infosec technologist working on usable technology development at Internews. She is passionate about making products usable and useful for communities who need them most.

SpeakerBio: Zach Singleton

No BIO available

Description:

Privacy isn't a one-size-fits-all solution and different perspectives, disciplines, and cultures are important considerations for giving consumers the choice & control they deserve—and the rights they are entitled to under the law. How can we bring new stakeholders to the table, build privacy controls users can find and understand, and hold companies accountable for respecting data rights?

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Rogues adventure & the intervillage badge

When: Sunday, Aug 9, 12:00 - 13:59 PDT

Where: Rogues Vlg

Speakers: Monero Village Team, Rogues Village Team

SpeakerBio: Monero Village Team

No BIO available

SpeakerBio: Rogues Village Team

No BIO available

Description:

You've played the game, now hear the story. ZY, the author of the Rogues Adventure (<http://www.foursuits.co/game>) will be here to answer your questions and talk about his journey in creating the adventure game, along with its integrations with the InterVillage Badge. Michael from Monero Village joins us to talk about the badge itself, and his collaborative process throughout its creation!

Rogues Village activities will be streamed via Twitch.

Twitch: <https://www.twitch.tv/roguesvillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: Rogues Village Introduction

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Rogues Vlg

SpeakerBio:Rogues Village Team

No BIO available

Description:

Who are we? What are we doing? How many ham-sandwiches can you fit into a handbag? Well, tune in to find out all of our secrets at Rogues Village this year.

Rogues Village activities will be streamed via Twitch.

Twitch: <https://www.twitch.tv/roguesvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Room for Escape: Scribbling Outside the Lines of Template Security

When: Thursday, Aug 6, 10:30 - 10:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Alvaro Munoz, Oleksandr Mirosh

SpeakerBio: Alvaro Munoz

Alvaro Muñoz (@pwntester) works as Staff Security Researcher with GitHub Security Lab. His research focuses on different programming languages and web application frameworks searching for vulnerabilities or unsafe uses of APIs. Before joining the research field, he worked as an Application Security Consultant helping enterprises to deploy their application security programs. Muñoz has presented at many Security conferences including Defcon, RSA, AppSecEU, Protect, DISCCON, etc and holds several InfoSec certifications, including OSCP, GWAPT and CISSP, and is a proud member of int3pids CTF team. Twitter: [@pwntester](#)

SpeakerBio: Oleksandr Mirosh , Software Security Researcher, Micro Focus Fortify

Oleksandr Mirosh has over 12 years of computer security experience, including vulnerability research, penetration testing, reverse engineering, fuzzing, developing exploits and consulting. He is working for Fortify Software Security Research team in Micro Focus investigating and analyzing new threats, vulnerabilities, security weaknesses, new techniques of exploiting security issues and development vulnerability detection, protection and remediation rules.

Twitter: [@olekmirosh](#)

Description:

Now more than ever, digital communication and collaboration are essential to the modern human experience. Shared digital content is everywhere and Content Management Systems (CMS) play a crucial role allowing users to design, create, modify and visualize dynamic content. In our research we discovered multiple ways to achieve Remote Code Execution (RCE) on CMS platforms through which an attacker can take full control of the resources your organization relies on.

Using a Microsoft SharePoint server as our main CMS attack surface, we combined flaws in its implementation and design with framework and language specific features to find six unique RCE vulnerabilities. In addition, we discovered ways to escape template sandboxes of the most popular Java Template engines and achieved RCE in many products including: Atlassian Confluence, Alfresco, Liferay, Crafter CMS, XWiki, Apache OfBiz, and more. We will analyze how these products and frameworks implement security controls and review the various techniques that we used to bypass them. We will describe all the vulnerabilities we uncovered in detail and show working demos of the most interesting attacks. Finally, we will present our general review methodologies for systems with dynamic content templates and provide practical recommendations to better protect them.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](#)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Running an appsec program with open source projects

When: Sunday, Aug 9, 13:00 - 13:45 PDT

Where: AppSec Vlg

SpeakerBio: Vandana Verma Sehgal

No BIO available

Twitter: [@InfosecVandana](#)

Description:

We are all heading towards the modernization of applications. However, we still see the companies being impacted with the most common website vulnerabilities like SQL Injection, Sensitive data exposure, security misconfiguration, etc.

OWASP has many projects which can be tied seamlessly into the application development pipeline structure. However, firstly we don't know if the projects exist, second, if we know about the projects, we do not know the exact working of the projects. In the talk, I will be talking about how to run an AppSec program with open source projects (OWASP Projects).

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Russian Cyber Threats in The Pandemic Era

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: BioHacking Vlg

SpeakerBio:Dr. Khatuna Mshvidobadze

Dr. Khatuna Mshvidobadze teaches cybersecurity and information management at Utica College and George Washington University. Her constantly updated “Russian Cyber Threats” has been presented around the world. Her articles have appeared throughout the international press.

Description:

Russia has seized upon the global Covid-19 pandemic as an opportunity to use its multifaceted, multidirectional information and cyberwarfare strategy against its prospective enemies. Russian state-sponsored hackers are using the coronavirus to spread different types of malware against western nations. Universities, hospitals and scientific facilities with access to classified information are targeted to steal data and research related to Covid-19. In this respect, the presentation will cover cyber-attack efforts against the healthcare industry in the United States and Europe. The presentation will discuss tactics, techniques and procedures (TTPs) of the advanced persistent threat (APT) groups. It will review Russian ransomware criminal actors and their communication channels (dark web).

The presentation also will highlight the role of the siloviki (people of power) in the country’s information warfare efforts. It will examine the structural units of the Russian Federal Security service (FSB) and Russian military intelligence (GRU), their projects and their networks of allied criminal groups. It will discuss how intelligence organizations are using APT groups through complex outsourcing strategies to conduct cyberwarfare over a broad spectrum. The presentation suggests several factors that drive the current trends in Russian cyber capabilities. It will also survey current trends: growing sophistication of TTPs and tools, supply chain threats, false flag operations, deception tactics, third party entry vectors and cyber espionage. Finally, the Russian Cyber Threat presentation will cover the role and mission of the Russian Foundation for Advanced Research Projects in the Defense Industry, the Russian Army’s Technopolis, and Russia’s chemical, biological, medical, informational and research efforts.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SaaSocalypse - The Complexity and Power of AWS Cross Account Access

When: Saturday, Aug 8, 14:45 - 15:30 PDT

Where: Cloud Vlg

SpeakerBio: Alexandre Sieira

Alexandre (or Alex) Sieira is a successful information security entrepreneur in the information security field with a global footprint since 2003. He began his security career as a Co-Founder and CTO of CIPHER, an international security consulting and MSSP headquartered in Brazil which was later acquired by Prosegur. In 2015, he became Co-Founder and CTO of Niddel, a bootstrapped security analytics SaaS startup running entirely on the cloud, which was awarded a Gartner Cool Vendor award in 2016. After the acquisition of Niddel by Verizon in January 2018, he became the Senior manager and global leader of the Managed Security Services - analytics products under the Detect & Respond portfolio tower at Verizon.

Currently is the Founder of Tenchi Security, a startup focused on cloud security headquartered in Brazil.

Alexandre is an experienced conference speaker in English and Brazilian Portuguese, with previous talks accepted at Black Hat, BSides San Francisco, FIRST Conference and local Latin American conferences.

Twitter: [@AlexandreSieira](https://twitter.com/AlexandreSieira)

Description:

AWS is a very complex and ever-changing platform, which presents a challenge to defenders and an opportunity for attackers. Among some of the most complex and powerful features of AWS is its IAM functionality, which allows for very granular control but is famously complex to learn and set up.

One the features of access control in AWS is that AWS accounts are a self-contained unit of processing, storage and access control. Given how AWS itself recommends segregation across accounts as a best practice, and the fact that many SaaS vendors request access to their customers' accounts in order to perform their services, this presents a challenge.

In this talk we will present in detail the policy-fu needed in order to securely allow principals from one account to perform actions on another, both inside different accounts in an organization but especially from the perspective of a SaaS provider that needs to access hundreds or thousands of customer accounts. Existing research on defenses and possible attacks will be presented and demonstrated to illustrate the concepts.

SaaS vendors like ""single pane of glass"" offerings, multi-cloud solutions and CSPM offerings are huge concentrators of risk since they have access to potentially thousands of customer AWS accounts. By exploring how this access can be uniquely secured due to capabilities only AWS provides and how vendors can fail at this we hope to allow attendees to better understand the risks of using these services, and also help service providers mitigate them.

YouTube: https://www.youtube.com/watch?v=gwBG_oKDINQ

#cloudv-general-text: <https://discord.com/channels/708208267699945503/732733373172285520>

[Return to Index](#) - Add to  - ics [Calendar file](#)

LPV - Sunday - 11:00-11:50 PDT

Title: Safecracking for Everyone!

When: Sunday, Aug 9, 11:00 - 11:50 PDT

Where: Lockpick Vlg

SpeakerBio:Jared Dygert

No BIO available

Description:

Safecracking is one of the more obscure type of lock in locksport. However, in most cases they can be manipulated without the need for any tools and opened in 5 minutes. This talk will get you an understanding of how that's done and started on your path to cracking your first safe!

Lockpick Village activities will be streamed to Twitch.

Twitch: https://www.twitch.tv/toool_us

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Satellite Orbits 101

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: Aerospace Vlg

SpeakerBio: Matt Murray

With a degree in Electrical and Computer Engineering at the undergraduate level and Computer Information Systems Engineering with concentrations in Networks and Cyber Security at the Graduate level; Matthew Murray has spent the last twelve of a twenty year career supporting aerospace, cyber and software engineering contracts with Lockheed Martin. His industry knowledge and expertise includes infrastructure hardware, software/hardware interfaces, software development, networking and cyber security. Throughout his career he has gained an in-depth understanding of an array of disciplines and technologies that include satellite orbits and the software development techniques tied to them.

Description:

Satellite Orbits 101 will provide an introductory understanding of the orbit of satellites/space vehicles. Leveraging knowledge, experience and visualization tools designed to describe and present orbital behaviors; the presentation will cover introductions to an array of orbital topics including what it even takes to reach and maintain orbit; which launch sites and windows are as important as they are; altitude classifications, such as HEO and LEO; directional classifications; inclination classifications, eccentricity classifications and more. The overlaps and interactions of these topics will also be discussed, as for example a satellite launched from near the equator and destined for a low-inclination orbit could receive help in reaching orbit from the rotation of the earth itself, but how this is not true for satellites bound for high inclination orbits. An attendee will walk away layman's introductory demystification of just how many layers are beneath the phrase Satellite Orbit.

This event will be coordinated on the DEF CON Discord server, in channel #av-space-text.

Discord: <https://discord.com/channels/708208267699945503/732394328105943180>

Return to Index - Add to  - ics [Calendar](#) file

DCG - Saturday - 13:15-13:59 PDT

Title: Saving Yourself from Microsoft: It's by design

When: Saturday, Aug 8, 13:15 - 13:59 PDT

Where: DEF CON Groups

Description:

Presentation by DC858 (San Diego, California, USA)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: SEATF: Maritime Hacking CTF

When: Friday, Aug 7, 06:00 - 15:59 PDT

Where: See Description or Village

Description:

Fathom5's Maritime-Industrial CTF event allows competitors to gain hands-on experience hacking real maritime hardware in a controlled environment using Fathom5's Grace maritime cybersecurity testbed. Grace is an accessible, realistic configuration of maritime systems where competitors complete challenges in a simulated afloat environment, with real ICS components and fieldbus protocols. The Grace testbed replicates a series of different maritime-industrial environments, including navigation, fire main, and hydraulic steering systems. The testbed makes both physical and simulated components available to competitors in order to replicate performance of maritime systems at lifelike scale. The CTF challenges scale from novice to expert-level on both IT and OT fronts such that competitors can gain experience on either side of the system. This CTF event has been deployed at DEFCON 27 (Aug 2019) as part of the Hack The Sea Village v1.0 and at HACKtheMACHINE-NYC (Sept 2019). It is also planned for to be deployed at DEFC ON 28 and HACKtheMACHINE-Atlanta in Aug 2020. This CTF can support approximately 20 teams of 3-5 individuals concurrently and typically takes 14 hours for skilled teams to navigate the challenges. The number of teams, size of teams, and depth of challenges can be adjusted to fit within host event timelines.

Forum: <https://forum.defcon.org/node/233012>

Discord: <https://discord.com/channels/708208267699945503/711644244753776640>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SEATF: Maritime Hacking CTF

When: Saturday, Aug 8, 06:00 - 15:59 PDT

Where: See Description or Village

Description:

Fathom5's Maritime-Industrial CTF event allows competitors to gain hands-on experience hacking real maritime hardware in a controlled environment using Fathom5's Grace maritime cybersecurity testbed. Grace is an accessible, realistic configuration of maritime systems where competitors complete challenges in a simulated afloat environment, with real ICS components and fieldbus protocols. The Grace testbed replicates a series of different maritime-industrial environments, including navigation, fire main, and hydraulic steering systems. The testbed makes both physical and simulated components available to competitors in order to replicate performance of maritime systems at lifelike scale. The CTF challenges scale from novice to expert-level on both IT and OT fronts such that competitors can gain experience on either side of the system. This CTF event has been deployed at DEFCON 27 (Aug 2019) as part of the Hack The Sea Village v1.0 and at HACKtheMACHINE-NYC (Sept 2019). It is also planned for to be deployed at DEFC ON 28 and HACKtheMACHINE-Atlanta in Aug 2020. This CTF can support approximately 20 teams of 3-5 individuals concurrently and typically takes 14 hours for skilled teams to navigate the challenges. The number of teams, size of teams, and depth of challenges can be adjusted to fit within host event timelines.

Forum: <https://forum.defcon.org/node/233012>

Discord: <https://discord.com/channels/708208267699945503/711644244753776640>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SEATF: Maritime Hacking CTF

When: Sunday, Aug 9, 06:00 - 15:59 PDT

Where: See Description or Village

Description:

Fathom5's Maritime-Industrial CTF event allows competitors to gain hands-on experience hacking real maritime hardware in a controlled environment using Fathom5's Grace maritime cybersecurity testbed. Grace is an accessible, realistic configuration of maritime systems where competitors complete challenges in a simulated afloat environment, with real ICS components and fieldbus protocols. The Grace testbed replicates a series of different maritime-industrial environments, including navigation, fire main, and hydraulic steering systems. The testbed makes both physical and simulated components available to competitors in order to replicate performance of maritime systems at lifelike scale. The CTF challenges scale from novice to expert-level on both IT and OT fronts such that competitors can gain experience on either side of the system. This CTF event has been deployed at DEFCON 27 (Aug 2019) as part of the Hack The Sea Village v1.0 and at HACKtheMACHINE-NYC (Sept 2019). It is also planned for to be deployed at DEFC ON 28 and HACKtheMACHINE-Atlanta in Aug 2020. This CTF can support approximately 20 teams of 3-5 individuals concurrently and typically takes 14 hours for skilled teams to navigate the challenges. The number of teams, size of teams, and depth of challenges can be adjusted to fit within host event timelines.

Forum: <https://forum.defcon.org/node/233012>

Discord: <https://discord.com/channels/708208267699945503/711644244753776640>

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 15:00-15:30 PDT

Title: Secretary Kim Wyman, Washington

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: Voting VIg

SpeakerBio: Kim Wyman , Secretary of State, Washington
No BIO available

Description: No Description available

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Secure Your Code — Injections and Logging

When: Sunday, Aug 9, 12:00 - 12:45 PDT

Where: AppSec Vlg

SpeakerBio: Philipp Krenn

No BIO available

Twitter: [@xeraa](#)

Description:

This talk combines two of the OWASP top ten security risks to highlight some widespread "this is fine" issues:

- Injections (A1:2017): We are using a simple application exploitable by injection and will then secure it with the Web Application Firewall (WAF) ModSecurity.
- Insufficient Logging & Monitoring (A10:2017): We are logging and monitoring both the secured and the unsecured application with the Elastic Stack.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Securing AND Pentesting the Great Spaghetti Monster (k8s)

When: Thursday, Aug 6, 09:15 - 10:15 PDT

Where: Red Team VIg

SpeakerBio: Kat Fitzgerald

Based in Pittsburgh and a natural creature of winter, you can typically find me sipping Grand Mayan Extra Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos. Honeypots & Refrigerators are a few of my favorite things! Fun Fact: I rescue Feral Pop Tarts and have the only Pop Tart Sanctuary in the Pittsburgh area.

Description:

We've all heard of it - Kubernetes - but do you really know what it is and, more importantly, how to set it up securely? The Great Spaghetti Monster isn't too difficult to secure if you just stop and use common sense (wait, WHAT?) security best practices. These techniques are for everyone - even those who have been playing with Kubernetes for some time.

Let's talk about Docker, baby!

You have to start somewhere, and containers are the place. Next, let's intro Kubernetes and the magic world of orchestration and what it really means to orchestrate containers. A quick recorded demo of my raspberry pi cluster will be shown here. As the brief Kubernetes demo concludes, it's time to bring in security by demonstrating the security plug-ins and tools used. Techniques are shown for best-in-show k8s security configuration. Remember this concept - "Common Sense ? Let's see if we can apply it with some best practices and build out the secure cluster. The focus on this is security threats to a Kubernetes cluster, containers and the apps deployed. A review of typical attack vectors in containers and Kubernetes clusters are shown with fun and exciting(?) pentesting tools specifically formulated for k8s. Now the fun begins - we have secured our cluster and our containers but how can we be sure? Let's put our blue-skills to the test with some red-skills and pentest our cluster. It's time to present some live security testing tools that are best suited for testing k8s. This is where the rubber meets the road, or in this case, where, wait for it — common sense prevails!!

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Saturday - 12:00-12:59 PDT

Title: Securing the COSMOS: How to operate and secure a validator

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Blockchain VIg

SpeakerBio:Ron Stoner

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Friday - 12:00-12:59 PDT

Title: Security Focused Operating System Design

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: Blockchain VIg

SpeakerBio: Colin Cantrell

No BIO available

Description: No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ETV - Friday - 16:00-16:59 PDT

Title: Security of Election Systems: A contract case study in progress

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: Ethics VIg

SpeakerBio: Rim Boujnah

No BIO available

Description:

This will be a live talk.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar file](#)

VMV - Friday - 12:30-12:59 PDT

Title: See Something, Say Something

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: Voting Vlg

SpeakerBio: Marten Mickos , CEO, HackerOne
No BIO available

Description: No Description available

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar file](#)

ENT - Friday - 23:00-23:59 PDT

Title: Shadowvex

When: Friday, Aug 7, 23:00 - 23:59 PDT

Where: See Description or Village

Description:

Underground hacker, audio/visual artist and researcher of entheogenic blockchain technology. ↯ Music is magick.

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Web: <https://shadowvex.com>

Twitter: <https://twitter.com/shadowvex>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Shrek, Juggs, and Toxic Trolls: a BADASS discussion about Online Sexuality and Hacktivism

When: Friday, Aug 7, 21:00 - 21:59 PDT

Where: DEF CON Fireside Twitch

Speakers: Katelyn Bowden, Rachel Lamp, Allie Barnes, Kate Venable, Marleigh Farlow, Tim Domsday

SpeakerBio: Katelyn Bowden , CEO and Founder, BADASS

No BIO available

SpeakerBio: Rachel Lamp , COO, BADASS

No BIO available

SpeakerBio: Allie Barnes , CTO, BADASS

No BIO available

SpeakerBio: Kate Venable , Head of Legal, BADASS

No BIO available

SpeakerBio: Marleigh Farlow , CMO, BADASS

No BIO available

SpeakerBio: Tim Domsday , CISO, BADASS

No BIO available

Description:

In this panel discussion, the BADASS army team will be talking about the intersection between security and sex, the problem of online exploitation and harassment, and what needs to be done to address these issues. After an introduction to the org and the culture of NOn Consensual Pornography, The panel will be a free form conversation with audience participation, covering a wide variety of topics related to NCP and online sexual abuse.

BADASS is a nonprofit org dedicated to fighting image based abuse. Founded in 2017 by victims of NCP, it has grown to be one of the major organizations trying to prevent online exploitation.

DEF CON Fireside Lounges will be live-streamed on Twitch.

Twitch: <https://www.twitch.tv/defconorg>

#fireside-lounge-text: <https://discord.com/channels/708208267699945503/738141986476916826>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Saturday - 10:00-10:59 PDT

Title: Single Board Computers in Amateur Radio

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Ham Radio Vlg

Description:

Have you ever tried Raspberry Pi and Ham together? It's a surprisingly good combination. In this talk, learn about how Raspberry Pis (and other single-board computers) play with ham radio.

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar file](#)

ENT - Saturday - 21:00-21:59 PDT

Title: Skittish & Bus

When: Saturday, Aug 8, 21:00 - 21:59 PDT

Where: See Description or Village

Description:

Married DJ/Producer duo, ↗† and hosts of underground dance music show Sonic Electronic.

@skittishandbus on instagram/twitter/facebook/soundcloud/mixcloud

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Twitter: <https://twitter.com/skittishandbus>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Friday - 14:00-14:59 PDT

Title: So You Got an SDR: Common Signals and the Wiki

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: Ham Radio Vlg

Description:

Come learn about how to use an software defined radio (SDR) to pick up and signals, and how to identify what they are and what they mean.

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Social Engineer SECTF4Teens

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231051>

Discord: <https://discord.com/channels/708208267699945503/726609125760434176>

Web: <https://www.social-engineer.org/sevillage-def-con/the-sectf4teens/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Social Engineer SECTF4Teens

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231051>

Discord: <https://discord.com/channels/708208267699945503/726609125760434176>

Web: <https://www.social-engineer.org/sevillage-def-con/the-sectf4teens/>

Return to Index - Add to  - ics [Calendar](#) file

Title: Social Engineer SECTF4Teens

When: Sunday, Aug 9, 00:00 - 15:59 PDT

Where: See Description or Village

Description:

Forum: <https://forum.defcon.org/node/231051>

Discord: <https://discord.com/channels/708208267699945503/726609125760434176>

Web: <https://www.social-engineer.org/sevillage-def-con/the-sectf4teens/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: SOHOpelessly Broken CTF

When: Saturday, Aug 8, 10:00 - 13:59 PDT

Where: See Description or Village

Description:

In this 3 time DEF CON Black Badge CTF hosted in IoT Village, players compete against one another by exploiting off-the-shelf IoT devices. These 25+ devices all have known vulnerabilities, but to successfully exploit these devices requires lateral thinking, knowledge of networking, and competency in exploit development. CTFs are a great experience to learn more about security and test your skills, so join up in a team (or even by yourself) and compete for fun and prizes! Exploit as many as you can during the con and the top three teams will be rewarded.

Forum: <https://forum.defcon.org/node/232897>

Discord: <https://discord.com/channels/708208267699945503/711644307597164665>

Twitter: <https://twitter.com/IoTvillage>

Web: <https://www.iotvillage.org/#yolo>

Return to Index - Add to  - ics [Calendar](#) file

Title: SOHOpelessly Broken CTF

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: See Description or Village

Description:

In this 3 time DEF CON Black Badge CTF hosted in IoT Village, players compete against one another by exploiting off-the-shelf IoT devices. These 25+ devices all have known vulnerabilities, but to successfully exploit these devices requires lateral thinking, knowledge of networking, and competency in exploit development. CTFs are a great experience to learn more about security and test your skills, so join up in a team (or even by yourself) and compete for fun and prizes! Exploit as many as you can during the con and the top three teams will be rewarded.

Forum: <https://forum.defcon.org/node/232897>

Discord: <https://discord.com/channels/708208267699945503/711644307597164665>

Twitter: <https://twitter.com/IoTvillage>

Web: <https://www.iotvillage.org/#yolo>

Return to Index - Add to  - ics [Calendar](#) file

Title: Sounds Legit: Why you shouldn't trust that speaker

When: Saturday, Aug 8, 21:30 - 22:30 PDT

Where: Red Team Vlg

Speakers:Luis Ángel Ramírez Mendoza (@larm182luis),Mauro Cáseres

SpeakerBio:Luis Ángel Ramírez Mendoza (@larm182luis)

Luis Ángel Ramírez Mendoza (@larm182luis) is a colombian electronic engineer, hacker and speaker. He spoke at DragonJAR Colombia (Biggest hacking spanish speaking conference in LATAM) and is currently working as a Cybersecurity and Artificial Intelligence Professor at University of Guajira in Colombia.

Twitter: [@larm182luis](https://twitter.com/larm182luis)

SpeakerBio:Mauro Cáseres

Mauro Cáseres (@mauroeldritch) is an argentine hacker and speaker. He spoke at DEF CON 26 Las Vegas (Recon & Data Duplication Villages), DevFest Siberia, DragonJAR Colombia, Roadsec Brasil, and DC7831 Nizhny Novgorod. Currently working as SecOps for the Argentine Ministry of Production.

Twitter: [@mauroeldritch](https://twitter.com/mauroeldritch)

Description:

BadUSB devices are popular worldwide, and almost no one ignores their nature: an object with a USB connection (usually a pendrive) connects to a computer and tells it "I am a keyboard", proceeding to send ("type") arbitrary commands, usually malicious. In this talk we have decided to go beyond the classic concept of a malicious pendrive. We use a set of classic USB speakers from a well-known brand available worldwide, which we disassemble to add our own hardware modification. This modification, which consists of cheap parts that can be acquired worldwide, makes this set of speakers an unprecedented local and remote attack vector: a device that looks and functions as a speaker, but is capable of acting as a keyboard, exfiltrate information, and use a SIM card to receive remote commands by telephone to leak information. When connected, the speaker passively waits for a phone call to its internal SIM from a specific number. Upon receiving it, launches a payload against the computer to which it was connected, allowing the attacker to obtain a shell. Now then, what would happen if someone left this speaker in its original box in a corner of an office? What would happen if someone connected this innocent device to their work terminal? Well, it is a speaker after all. And it definitely sounds legit...

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Spectra—New Wireless Escalation Targets

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: DEF CON Q&A Twitch

Speakers: Francesco Gringoli, Jiska Classen

SpeakerBio: Francesco Gringoli , University of Brescia

No BIO available

SpeakerBio: Jiska Classen , Secure Mobile Networking Lab

jiska likes to break things, and Francesco loves reverse engineering. They both have a history in binary patching on Broadcom chips. While jiska focuses on the Bluetooth side of this project, Francesco is the Wi-Fi specialist.

Twitter: [@naehrdine](https://twitter.com/naehrdine)

Description:

Wireless coexistence enables high-performance communication on platforms with a small form factor despite overlapping frequency bands. On-chip coexistence is essential to combine wireless technologies, and manufacturers implement various proprietary solutions. This presentation demonstrates multiple attacks on two coexistence features of Broadcom and Cypress Wi-Fi/Bluetooth combo chips. Various popular devices that were released over a decade are affected, such as the Google Nexus 5 and iPhone 6, but also the newest iPhone 11 and Samsung Galaxy S20.

On the analyzed chips, Wi-Fi and Bluetooth run on separate processing cores, but various information leaks and even code execution become possible through their coexistence interfaces. As these escalations concern an internal chip interface, the operating system cannot prevent them. However, coexistence exploitation widens the possibilities to escalate into drivers and the operating system on top.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](https://discord.com/channels/708208267699945503/733079621402099732)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

AIV - Friday - 13:30-13:59 PDT

Title: Spectrum: An End-to-End Framework for ML-based Threat Monitoring and Detection

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: AI Vlg

SpeakerBio: Nahid Farhady

No BIO available

Description: No Description available

AI Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/aivillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HTS - Saturday - 10:00-10:59 PDT

Title: Speed 2: The Poseidon Adventure – When Cruise Ships Go Wrong

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Hack the Sea Vlg

SpeakerBio: Andrew Tierney

No BIO available

Description: No Description available

Hack the Sea Village activities will be streamed to Twitch.

Twitch: <https://twitch.tv/hackthesea>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Starkiller

When: Sunday, Aug 9, 12:00 - 13:50 PDT

Where: See Description or Village

Description:

The ultimate goal for any security team is to increase resiliency within an organization and adapt to the modern threat. Starkiller aims to provide red teams with a platform to emulate Advanced Persistent Threat (APT) tactics. Starkiller is a frontend for the post-exploitation framework, PowerShell Empire, which incorporates a multi-user GUI application that interfaces with a remote Command and Control (C2) server. Empire is powered by Python 3 and PowerShell and includes many widely used offensive security tools for Windows, Linux, and macOS exploitation. The framework's flexibility to easily incorporate new modules allows for a single solution for red team operations. Both red and blue teams can utilize Starkiller to emulate and defend against the most used APT attack vectors.

Audience: Offense, Defense

Interact @ #dl-rose-starkiller-text: <https://discord.com/channels/708208267699945503/730256356292165682>

Watch @ #dl-video2-voice: <https://discord.com/channels/708208267699945503/734027778646867988>

Web: <https://www.bc-security.org/post/an-introduction-to-starkiller>

Forum: <https://forum.defcon.org/node/233126>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Starkiller

When: Saturday, Aug 8, 10:00 - 11:50 PDT

Where: See Description or Village

SpeakerBio: Vincent "Vinnybod" Rose

Vincent "Vinnybod" Rose is a software engineer with experience in cloud services. He has a decade of experience in software development and networking. Recently, his focus has been on building ad-serving technologies, web and server-side applications. He is the lead developer for Starkiller, the graphical user interface for the Empire framework.

Description:

The ultimate goal for any security team is to increase resiliency within an organization and adapt to the modern threat. Starkiller aims to provide red teams with a platform to emulate Advanced Persistent Threat (APT) tactics. Starkiller is a frontend for the post-exploitation framework, PowerShell Empire, which incorporates a multi-user GUI application that interfaces with a remote Command and Control (C2) server. Empire is powered by Python 3 and PowerShell and includes many widely used offensive security tools for Windows, Linux, and macOS exploitation. The framework's flexibility to easily incorporate new modules allows for a single solution for red team operations. Both red and blue teams can utilize Starkiller to emulate and defend against the most used APT attack vectors.

Audience: Offense, Defense

Interact @ #dl-rose-starkiller-text: <https://discord.com/channels/708208267699945503/730256356292165682>

Watch @ #dl-video1-voice: <https://discord.com/channels/708208267699945503/734027693250576505>

Web: <https://www.bc-security.org/post/an-introduction-to-starkiller>

Forum: <https://forum.defcon.org/node/233126>

Return to Index - Add to  - ics [Calendar](#) file

Title: STARTTLS is Dangerous

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio:Hanno Böck

Hanno is a freelance writer and IT security professional. He has discovered high profile TLS vulnerabilities in the past, including the ROBOT attack and flaws in TLS GCM implementations. He is the author of the monthly Bulletproof TLS Newsletter.

Description:

The STARTTLS mechanism allows upgrading insecure protocols to a TLS encrypted connection. This mechanism is incredibly fragile and almost by default leads to vulnerable implementations. In 2011 Wietse Venema discovered a flaw in Postfix that allowed a man in the middle attacker to inject commands into an encrypted connection [1].

We discovered that the flaw is still widely present in E-Mail servers and also, previously unknown, the same flaw exists in many mail clients. In some cases these flaws allow stealing E-Mail credentials. Furthermore the STARTTLS mechanism is weakly specified and in part contradictory, which allows other attacks.

The talk will give an overview on why STARTTLS is dangerous and should be avoided.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Static analysis of Infrastructure as code: Terraform, Kubernetes, Cloudformation and more!

When: Friday, Aug 7, 12:50 - 13:25 PDT

Where: Cloud Vlg

SpeakerBio:Barak Schoster

Barak Schoster is CTO and Co-founder at Bridgecrew, working from Tel Aviv, Israel, Helping teams secure cloud infrastructure. Often contributing to open source projects including Checkov, AirIAM, Terragoat, Prowler, and others. He has previously worked for RSA focused on cybersecurity machine learning and big data architecture as well as at Fortscale and IDF tech unit. When not writing code or Barak loves to drink coffee and wine (but not at the same time).

Twitter: [@BarakSchoster](https://twitter.com/BarakSchoster)

Description:

Planning, provisioning, and changing infrastructure are becoming vital to rapid cloud application development. Incorporating infrastructure-as-code into software development promotes transparency and immutability and helps prevent bad configurations upstream.

About this talk: Planning, provisioning, and changing infrastructure are becoming vital to rapid cloud application development. Incorporating infrastructure-as-code into software development promotes transparency and immutability and helps prevent bad configurations upstream.

In this talk:

We'll cover the current state of infrastructure security in the open source registries.

From there we will continue to discuss best practices for writing, testing, and maintaining infrastructure at scale, keeping the infrastructure code secured using open source scanners.

We will cover infrastructure security use cases like encryption, public-facing data entities and plain text secrets, And will show how to find those using policy as code.

Based on the open source tool:

<https://github.com/bridgecrewio/checkov/tree/master/docs>

And the training resources:

<https://github.com/bridgecrewio/terragoat/> <https://github.com/madhuakula/kubernetes-goat>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Stepped on a Nail

When: Saturday, Aug 8, 18:00 - 18:45 PDT

Where: IOT Vlg

SpeakerBio: Matthew Byrdwell

Matthew Byrdwell ("Nerdwell") is passionate about securing the Internet and helping others achieve their infosec career goals. He's been building and breaking IT systems for 20 years and currently works in Critical Infrastructure Protection. He enjoys doing cybersecurity research, both independently and through bug bounty programs, and contributes to the community as a Bugcrowd Ambassador.

Description:

It was a crisp October evening as Nerdwell walked the streets of the Internet looking for juicy bugs. Suddenly, his attention was drawn to something that he could not ignore. "Is that memory?" He thought to himself, "it sure is ... a whole heap of it!"

In this talk, Nerdwell will share the story of how a chance observation, along with healthy doses of curiosity and persistence, ultimately led to a high severity finding of unauthenticated remote memory disclosure in the Mitel MiVoice 6800 and 6900 series SIP Phones. Nerdwell will take us through the technical details of CVE-2020-13617 and demonstrate exploitation. He'll then share some of the insights gained along the way, including:

- Unexpected benefits of the emerging bug bounty industry upon IoT security in general;
- The roles of curiosity and creativity in the hacker's mindset, and how these traits influence security research; and
- Ways to use open source tools, like Shodan.io and GitHub, to select IoT devices for further research.

The talk will close with suggestions for future research and tips for new researchers looking to break into the field of IoT hacking.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Subxian

When: Saturday, Aug 8, 23:00 - 23:59 PDT

Where: See Description or Village

Description:

LA/Seattle Underground Music 1997-present. DEF CON SoundGuy. Moontribe collective. So,many parties and so much good music made me picky but I love halftime beats! Twice as much opportunity for intricate layers!

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

[Return to Index](#) - Add to  - ics [Calendar](#) file

BTWV1 - Thursday - 16:15-16:59 PDT

Title: Suricata: An Introduction Into OpenSOC CTF Tools

When: Thursday, Aug 6, 16:15 - 16:59 PDT

Where: Blue Team VIg - Workshop Track 1

SpeakerBio:Josh

No BIO available

Description:

Every year the Blue Team Village hosts OpenSOC. A unique defense CTF meant to teach and test practical incident response skills in an environment that's as close to "the real thing" as it gets.

This year BTV wanted to do more. We know that some Blue Teamers might be unfamiliar with some of the tools used by OpenSOC. And we didn't want that to keep anyone from playing this incredible defense simulation.

So this year we are dedicating all day Thursday to demo the various OpenSOC tools, before OpenSOC starts on Friday. These are tools like Graylog, Moloch, Zeek, Osquery, and others that Blue Teamers rely on every day to defend their networks against attackers.

That means that after you LEARN the tools, you can PLAY the OpenSOC CTF, and then take that knowledge back to your own Blue Team to DO the work of defending your network.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Take Down the Internet! With Scapy

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: Packet Hacking VIg - Talk

SpeakerBio:C8 (John Hammond)

John Hammond (Twitter: @_johnhammond) is a cybersecurity instructor, developer, red teamer, and CTF enthusiast. Cyber Training Academy curriculum developer and teacher for the Cyber Threat Emulation course, educating both civilian and military members on offensive Python, PowerShell, other scripting languages and the adversarial mindset. He personally developed training material and infosec challenges for events such as PicoCTF and the "Capture the Packet" competition at DEFCON US. John speaks at security conferences such as BsidesNoVA, to students at colleges such as the University of North Carolina Greensboro, and other events like the SANS Holiday Hack Challenge/KringleCon. He is an online YouTube personality to showcase programming tutorials, cyber security guides, and CTF video walkthroughs. John currently holds the following certifications: Security+, eJPT, CEH, PCAP, OSWP, OSCP, OSCE, and OSWE.

Twitter: [@_johnhammond](https://twitter.com/_johnhammond)

Description:

You know Python remains a hacker's favorite language... and for both network defenders and attackers alike, Scapy shines as their favorite Python module! This talk introduces Scapy and its syntax, discusses and showcases multiple attacks that can be performed with Scapy (SYN flood, Ping of Death, DNS amplification attacks and more) as well as offering some defensive techniques to mitigate these attacks. These network attacks are often a "denial of service" and have dire consequences – so you choose your role as an attacker or defender, and be part of either the cause or the solution to take down the Internet!

YouTube: <http://youtube.com/wallofsheep>

Twitch: <http://twitch.tv/wallofsheep>

Facebook: <http://facebook.com/wallofsheep/>

Periscope: <https://t.co/gn17JLftA?amp=1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Friday - 11:00-11:59 PDT

Title: Talking to Satellites

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Ham Radio Vlg

Description:

Reaching out into space may seem like it would require a PhD and thousands of dollars of equipment, but it can actually be done for about \$100. In this talk I will detail how to get started talking to satellites using basic equipment. With just a Ham Radio license and some gear, you too can talk to satellites and by extension people thousands of miles away.

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Talking To Satellites - 101

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: Aerospace Vlg

SpeakerBio:Eric Escobar

Eric is a seasoned pentester and a Principal Security Consultant at Secureworks. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. He has successfully compromised companies from all sectors of business including: Healthcare, Pharmaceutical, Entertainment, Amusement Parks, Banking, Finance, Technology, Insurance, Retail, Food Distribution, Government, Education, Transportation, Energy and Industrial Manufacturing.

His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he now helps create challenges!

Description:

Reaching out into space may seem like it would require a PhD and thousands of dollars of equipment, but it can actually be done for about \$100. In this talk I will detail how to get started talking to satellites using basic equipment. With just a Ham Radio license and some gear, you too can talk to satellites and by extension people thousands of miles away.

This event will be coordinated on the DEF CON Discord server, in channel #av-space-text.

Discord: <https://discord.com/channels/708208267699945503/732394328105943180>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: TechCongress

When: Saturday, Aug 8, 16:30 - 17:40 PDT

Where: Ethics VIg

SpeakerBio:Leisel Bogan

No BIO available

Description:

This will be a 40-minute pre-recorded talk, followed by a 30-minute live Q&A session.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: TeleChallenge

When: Friday, Aug 7, 09:00 - 23:59 PDT

Where: See Description or Village

Description:

It's Election 2020! The national vote-by-phone polls are about to open and it's a knock down, drag-out battle of political wits between Presidential candidates Michael Key and Founder Jack Carson, VC. DEF CON hackers, team up and take to the phones: lie, cheat, and steal your way to the ultimate victory. Every hacker vote counts—so vote early and often!

Forum: <https://forum.defcon.org/node/231949>

Discord: <https://discord.com/channels/708208267699945503/711644470063399012>

Twitter: <https://twitter.com/TeleChallenge>

Web: <https://telechallenge.org>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: TeleChallenge

When: Saturday, Aug 8, 00:00 - 23:59 PDT

Where: See Description or Village

Description:

It's Election 2020! The national vote-by-phone polls are about to open and it's a knock down, drag-out battle of political wits between Presidential candidates Michael Key and Founder Jack Carson, VC. DEF CON hackers, team up and take to the phones: lie, cheat, and steal your way to the ultimate victory. Every hacker vote counts—so vote early and often!

Forum: <https://forum.defcon.org/node/231949>

Discord: <https://discord.com/channels/708208267699945503/711644470063399012>

Twitter: <https://twitter.com/TeleChallenge>

Web: <https://telechallenge.org>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: TeleChallenge

When: Sunday, Aug 9, 00:00 - 11:59 PDT

Where: See Description or Village

Description:

It's Election 2020! The national vote-by-phone polls are about to open and it's a knock down, drag-out battle of political wits between Presidential candidates Michael Key and Founder Jack Carson, VC. DEF CON hackers, team up and take to the phones: lie, cheat, and steal your way to the ultimate victory. Every hacker vote counts—so vote early and often!

Forum: <https://forum.defcon.org/node/231949>

Discord: <https://discord.com/channels/708208267699945503/711644470063399012>

Twitter: <https://twitter.com/TeleChallenge>

Web: <https://telechallenge.org>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: tense future

When: Saturday, Aug 8, 18:00 - 18:59 PDT

Where: See Description or Village

Description:

Los Angeles, CA. Trapped in an autonomous car during a solar flare. Anxiety attack over spying home appliances that tip their hand. General AI caretaker grappling over competing logical fallacies. Dark techno sounds from the tense future that was once distant.

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Soundcloud: <https://soundcloud.com/tensefuture>

Twitter: <https://twitter.com/tensefutur3>

Return to Index - Add to  - ics [Calendar](#) file

ENT - Friday - 18:00-18:59 PDT

Title: Terrestrial Access Network

When: Friday, Aug 7, 18:00 - 18:59 PDT

Where: See Description or Village

Description:

If packets could dance, they would surely dance to this...

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Twitch: https://www.twitch.tv/defcon_music

Soundcloud: <https://soundcloud.com/collinsullivan>

Spotify: <https://open.spotify.com/artist/53WcPPzAkgtrcJhAfytwMN>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: The Art of Balancing: A Burnout Talk

When: Saturday, Aug 8, 14:15 - 14:59 PDT

Where: Red Team VIg

SpeakerBio:Chloé Messdaghi

Chloé Messdaghi is the VP of Strategy at Point3 Security. She is a security researcher advocate who strongly believes that information security is a humanitarian issue. Besides her passion to keep people safe and empowered online & offline, she is driven to fight for hacker rights. She is the founder of WomenHackerz & the President and cofounder of Women of Security (WoSEC), podcaster for ITSP Magazine's The Uncommon Journey, and runs the Hacker Book Club.

Description:

Mental health is an ongoing issue within infosec before and during COVID-19. There's a fine balance between hacking and personal life. Majority of the time, they cross over. This talk shares an overview of the warning signs, symptoms, and practices to prevent burnout and how to deal with burnout to keep balanced.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: Voting VIg

SpeakerBio: Michael A. Specter , EECS PhD Candidate, Massachusetts Institute of Technology (MIT)

No BIO available

Description:

In the 2018 midterm elections, West Virginia became the first state in the U.S. to allow select voters to cast their ballot on a mobile phone via a proprietary app called “Voatz. Although there was no public formal description of Voatz’s security model, the company claimed that election security and integrity were maintained through the use of a permissioned blockchain, biometrics, a mixnet, and hardware-backed key storage modules on the user’s device. In this work, we present the first public security analysis of Voatz, based on a reverse engineering of their Android application and the minimal available documentation. We performed a cleanroom reimplementaion of Voatz’s server and present an analysis of the election process as visible from the app itself.

We find that Voatz has vulnerabilities that allow different kinds of adversaries to alter, stop, or expose a user’s vote, including a sidechannel attack in which a completely passive network adversary can recover a user’s secret ballot. We additionally find that Voatz has a number of privacy issues stemming from their use of third party services for crucial app functionality. Our findings serve as a concrete illustration of the common wisdom against Internet voting, and of the importance of transparency to the legitimacy of elections.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Basics Of Breaking BLE v3

When: Thursday, Aug 6, 09:00 - 09:01 PDT

Where: Wireless Vlg

SpeakerBio: FreqyXin

Maxine is a US Army Veteran, and recent graduate from the University of Washington – Tacoma completing a degree in Information Assurance and Cybersecurity. She has experience as a Security Analyst hunting wireless threats and vulnerabilities, and currently works for IOActive as a Security Consultant applying her knowledge to help companies identify wireless risks within their environments and products. She has taught wireless security concepts as a guest lecturer at the University of Washington, a speaker at industry conferences, and as an outside consultant for the US Army. Maxine was also selected for the SANS Women's Immersion Academy 2018 Cohort and holds the GSEC, GCIH, and GPEN GIAC certifications.

Description:

Evolving over the past twenty-two years, Bluetooth, especially Bluetooth Low Energy (BLE), has become the ubiquitous backbone modern devices use to perform low energy communications. From mobile, to IoT, to Auto, most smart devices now support Bluetooth connections, meaning that the attack vector is becoming an increasingly important aspect of security testing. This talk will breakdown the various phases of testing Bluetooth devices with an emphasis on sniffing BLE connections, spoofing devices, and exploiting GATT services. We will cover key components of the Bluetooth protocol stack, and the tools required to start testing BLE in your home, or as part of a Bluetooth pentest. This talk will also demonstrate that all you need to start testing BLE is an Android or iOS device, and a bit of curiosity.

This talk is available on YouTube.

Talk: <https://www.youtube.com/watch?v=7giQCeNBJek>

Return to Index - Add to  - ics [Calendar](#) file

Title: The Bug Hunter's Methodology

When: Thursday, Aug 6, 08:00 - 08:59 PDT

Where: Red Team VIg

SpeakerBio: Jason Haddix

Jason Haddix is the Head of Security for a leading videogame production company. Previously he was VP of Trust and Security at Bugcrowd and currently holds the 29th all-time ranked researcher position. Before joining Bugcrowd Jason was the Director of Penetration Testing for HP Fortify and also held the #1 rank on the Bugcrowd leaderboard for two years. He is a hacker and bug hunter through and through and specializes in recon and web application analysis. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason lives in Colorado with his wife and three children.

Description:

The Bug Hunter's Methodology is an ongoing yearly installment on the newest tools and techniques for bug hunters and red teamers. This version explores both common and lesser-known techniques to find assets for a target. The topics discussed will look at finding a targets main seed domains, subdomains, IP space, and discuss cutting edge tools and automation for each topic. By the end of this session a bug hunter or red team we will be able to discover and multiply their attack surface. We also discuss several vulnerabilities and misconfigurations related to the recon phase of assessment.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 12:00-12:45 PDT

Title: The DevOps & Agile Security Toolkit

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: AppSec Vlg

SpeakerBio:David Waldrop

No BIO available

Description:

The DevOps & Agile Security Toolkit - In this talk, we will look at integrating security into Agile and DevOps. We will discuss strategies, training, tools, and techniques that will let your organization move quickly while doing so safely.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8Ll0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Elephant in the Room: Burnout

When: Sunday, Aug 9, 10:00 - 10:45 PDT

Where: AppSec Vlg

SpeakerBio:Chloé Messdaghi

Chloé Messdaghi is the VP of Strategy at Point3 Security. She is a security researcher advocate who strongly believes that information security is a humanitarian issue. Besides her passion to keep people safe and empowered online & offline, she is driven to fight for hacker rights. She is the founder of WomenHackerz & the President and cofounder of Women of Security (WoSEC), podcaster for ITSP Magazine's The Uncommon Journey, and runs the Hacker Book Club.

Description:

Burnout. We all go through it at one point, especially during a pandemic. It feels like you are low on battery and it can cause emotional and physical issues. This talk shares an overview of the warning signs, symptoms, and practices to prevent burnout and how to deal with burnout to keep balanced.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The future of IoT Security “Baselines, Standards, and Regulatory Domain

When: Saturday, Aug 8, 14:30 - 15:20 PDT

Where: IOT Vlg

Speakers: Amit Elazari, Anahit Tarkhanyan

SpeakerBio: Amit Elazari

Dr. Amit Elazari is a Director, Global Cybersecurity Policy at Intel Corporation and a Lecturer at UC Berkeley’s School of Information Master in Information and Cybersecurity. She holds a Doctoral Degree in the Law (J.S.D.) from UC Berkeley School of Law and graduated summa cum laude three prior degrees. Her research in information security law and policy has appeared in leading technology law and computer science journals, presented at conferences such as RSA, Black Hat, USENIX Enigma, USENIX Security, BsidessLV, BsidessSF and DEF CON Villages, and featured at leading news sites such as The Wall Street Journal, The Washington Post and the New York Times. In 2018, she received a Center for Long Term Cybersecurity grant for her work on private ordering regulating information security, exploring safe harbors for security researchers. She practiced law in Israel.

SpeakerBio: Anahit Tarkhanyan

Anahit Tarkhanyan is Platform Architect at Intel and leads IoT hardware-based security product architecture. She joined Intel in 2011 and has over 20 years of industry experience delivering security solutions to the market. Her area of expertise covers silicon-based Edge to Cloud systems security and AI/ML protection. Anahit is a recognized contributor to Intel’s hardware security and a trusted advisor for ecosystem partners. She has PhD in Distributed Computer Systems and Networks, holds several patents, and has publications in diverse security technology areas.

Description:

Security is one of the most dynamic and impactful landscapes in the regulatory sphere. Proposed initiatives and standards in IoT security specifically, are shaping the industry at a fast pace and on a global scale. With the potential for marked impact to the researcher community, this evolving landscape also serves as an opportunity for technology innovation and collaboration. This talk, a joint presentation from policy expert, Dr. Amit Elazari, and IoT platform architect, Anahit Tarkhanyan, will introduce the audience to a variety of regulatory concepts and baseline proposals shaping the future of IoT security. They’ll focus on recent trends including: NISTIR 8259, C2, international standards, supply chain transparency, researchers’ collaboration, proposed legislation, Coordinated Vulnerability Disclosure, and the innovative, technical capabilities that can support and enhance development from the foundation up.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Gold Bug – Crypto and Privacy Village Puzzle

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle will keep you intrigued and busy throughout Defcon - and questioning how deep the layers of cryptography go.

The Gold Bug an annual Defcon puzzle hunt, 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. Accessible to all - and drop by for some kids' puzzles too! **PELCGBTENCUL VF UNEQ**

Forum: <https://forum.defcon.org/node/232942>

Discord: <https://discord.com/channels/708208267699945503/711644108837486602>

Twitter: <https://twitter.com/CryptoVillage>

Web: <https://goldbug.cryptovillage.org/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Gold Bug – Crypto and Privacy Village Puzzle

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle will keep you intrigued and busy throughout Defcon - and questioning how deep the layers of cryptography go.

The Gold Bug an annual Defcon puzzle hunt, 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. Accessible to all - and drop by for some kids' puzzles too! **PELCGBTENCUL VF UNEQ**

Forum: <https://forum.defcon.org/node/232942>

Discord: <https://discord.com/channels/708208267699945503/711644108837486602>

Twitter: <https://twitter.com/CryptoVillage>

Web: <https://goldbug.cryptovillage.org/>

Return to Index - Add to  - ics [Calendar](#) file

Title: The Gold Bug – Crypto and Privacy Village Puzzle

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle will keep you intrigued and busy throughout Defcon - and questioning how deep the layers of cryptography go.

The Gold Bug an annual Defcon puzzle hunt, 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. Accessible to all - and drop by for some kids' puzzles too! **PELCGBTENCUL VF UNEQ**

Forum: <https://forum.defcon.org/node/232942>

Discord: <https://discord.com/channels/708208267699945503/711644108837486602>

Twitter: <https://twitter.com/CryptoVillage>

Web: <https://goldbug.cryptovillage.org/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Individual Contributor to Tech Executive, or There and Back Again

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: Career Hacking Vlg

SpeakerBio: Amelie Koran

No BIO available

Description:

It's common perceived expectation that you're expected to move from an individual contributor on a team to eventually a senior leadership role, if given time an interest, but what works for somebody else may not work for you based on interests, changes in career demands, as well as life in general. Following a similar role, I'd like to impart how, like the Hobbit's journey, explore, adventure and challenges will forge a life you can be proud of and be able to live to tell the tale.

Audience: This presentation is geared towards all levels of attendees, entry to senior-level professionals. It's a discussion on the journey, a "lessons learned but also novel perspectives given experiences in multiple roles and industries, both private and public sectors. Also, as an LGBTQ+ community member, I will offer a rather unique perspective on the challenge of career development and advancement within multiple "ceilings .

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Friday - 13:45-14:45 PDT

Title: The Journey of ICS Project Files - Visibility and Forensics to Exploitation

When: Friday, Aug 7, 13:45 - 14:45 PDT

Where: ICS V1g

SpeakerBio: Nadav Erez

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Joy of Coordinating Vulnerability Disclosure

When: Friday, Aug 7, 18:30 - 19:15 PDT

Where: IOT VIg

Speakers: Daniel Gruss, CRob, Lisa Bradley, Katie Noble, Omar Santos, Anders Fogh

SpeakerBio: Daniel Gruss , TU Graz

No BIO available

SpeakerBio: CRob , Red Hat

No BIO available

SpeakerBio: Lisa Bradley , Dell

No BIO available

SpeakerBio: Katie Noble , Intel Corp

Katie currently serves as a Director of PSIRT and Bug Bounty at Intel Corp. Where she leads the cyber security vulnerability Bug Bounty program, researcher outreach, and strategic planning efforts. Previous to this position, Katie served as the Section Chief of the Vulnerability Management and Coordination at the Department of Homeland Security, Cyber and Infrastructure Security Agency (CISA) where she led DHS' primary operations arm for coordinating the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems, enterprise, hardware and software. Katies team is credited by the Secretary of Homeland Security with the coordination and public disclosure of over 20,000 cyber security vulnerabilities within a two year period. Katie is a highly accomplished manager with over 14 years of U.S. Government experience, both in the Intelligence Community and Cyber Security Program Management. She has operated at all levels from individual contributor as an Intelligence Analyst for the National Intelligence Community to Senior Policy Advisor for White House led National Security Council (NSC) Cyber programs. Her work has directly impacted the decision making of the NSC, Defense Information Systems Agency, Office of the Director of National Intelligence, Department of Defense, Federal Communications Commission, Central Intelligence Agency, U.S. Coast Guard, U.K. Ministry of Defense, Canadian Government agencies, and Australian Cabinet Ministry.

SpeakerBio: Omar Santos , Cisco

Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure. Omar is the author of over 20 books and video courses; numerous white papers, and other articles. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities. Omar is often presenting at many conferences and he is the co-lead of the DEF CON Red Team Village.

Twitter: [@santosomar](https://twitter.com/santosomar)

SpeakerBio: Anders Fogh , Intel

No BIO available

Description:

Under the best of circumstances, coordinating disclosure of vulnerabilities can be a challenge. At times it can feel like everyone involved in CVD has conflicting motivations. The truth is that all of us are aspiring to do the right thing for end-users based on our perspective. The panel will share experiences and show how researchers and technology companies can work together to improve the impact of disclosing vulnerabilities on the technology ecosystem. Join CRob (Red Hat), Lisa Bradley (Dell), Katie Noble (Intel), Omar Santos (Cisco), Anders Fogh (Intel) and Daniel Gruss (TU Graz) for an exciting and engaging dialog between security researchers and industry experts on the Joy of coordinating vulnerability disclosure.

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar file](#)

HRV - Sunday - 10:00-11:30 PDT

Title: The K0BAK Rover Van

When: Sunday, Aug 9, 10:00 - 11:30 PDT

Where: Ham Radio Vlg

Description:

Come see how Pete (K0BAK) is converting an old TV news station van, the kind used to produce and relay live TV reporting, into a mobile ham radio station!

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: The Norwegian Blue: A lesson in Privacy Engineering

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Eivind Arvesen

Eivind is a senior software developer and architect who works as a consultant for Bouvet, specializing in security and privacy. He holds a master's degree with a focus on machine learning, and has experience ranging from his own startup during his studies to large organizations both public and private. Eivind was recently temporarily pulled from his usual project within critical infrastructure to be part of a government appointed expert panel tasked with evaluating the Norwegian COVID-19 app. In his spare time, Eivind writes about privacy issues, participates in bug bounties, contributes to open source software and records music.

Description:

"Can smartphones automate contact tracing?" As COVID-19 spread like wildfire earlier this year, health authorities around the world asked themselves this question. If so: What data would you need, from whom, under what circumstances – and which safeguards should be in place? You could just upload all of everyone's data from every sensor continuously, right? It's not like you know for certain what data you'll need anyways. Besides, people should trust their government. What could go possibly wrong? Join me as I explore how Norway became worst-in-class in contact tracing. I'll be telling the story of how I became a member of the government appointed expert panel tasked with evaluating the Norwegian COVID-19 app, what we found, as well as the weirdness that unfolded around us before, during, and after our work.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

Return to Index - Add to  - ics [Calendar](#) file

Title: The Schemaverse Championship

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The Schemaverse [skee-muh vurs] is a space battleground that lives inside a PostgreSQL database. Mine the hell out of resources and build up your fleet of ships, all while trying to protect your home planet. Once you're ready, head out and conquer the map from other DEF CON rivals.

This unique game gives you direct access to the database that governs the rules. Write SQL queries directly by connecting with any supported PostgreSQL client or use your favourite language to write AI that plays on your behalf. This is DEF CON of course so start working on your SQL Injections - anything goes!

Forum: <https://forum.defcon.org/node/233021>

Discord: <https://discord.com/channels/708208267699945503/711644182116040784>

Twitter: <https://twitter.com/schemaverse>

Web: <https://schemaverse.com>

Return to Index - Add to  - ics [Calendar](#) file

Title: The Schemaverse Championship

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The Schemaverse [skee-muh vurs] is a space battleground that lives inside a PostgreSQL database. Mine the hell out of resources and build up your fleet of ships, all while trying to protect your home planet. Once you're ready, head out and conquer the map from other DEF CON rivals.

This unique game gives you direct access to the database that governs the rules. Write SQL queries directly by connecting with any supported PostgreSQL client or use your favourite language to write AI that plays on your behalf. This is DEF CON of course so start working on your SQL Injections - anything goes!

Forum: <https://forum.defcon.org/node/233021>

Discord: <https://discord.com/channels/708208267699945503/711644182116040784>

Twitter: <https://twitter.com/schemaverse>

Web: <https://schemaverse.com>

Return to Index - Add to  - ics [Calendar](#) file

Title: The Schemaverse Championship

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

The Schemaverse [skee-muh vurs] is a space battleground that lives inside a PostgreSQL database. Mine the hell out of resources and build up your fleet of ships, all while trying to protect your home planet. Once you're ready, head out and conquer the map from other DEF CON rivals.

This unique game gives you direct access to the database that governs the rules. Write SQL queries directly by connecting with any supported PostgreSQL client or use your favourite language to write AI that plays on your behalf. This is DEF CON of course so start working on your SQL Injections - anything goes!

Forum: <https://forum.defcon.org/node/233021>

Discord: <https://discord.com/channels/708208267699945503/711644182116040784>

Twitter: <https://twitter.com/schemaverse>

Web: <https://schemaverse.com>

Return to Index - Add to  - ics [Calendar](#) file

Title: The Student Roadmap to Becoming A Penetration Tester

When: Saturday, Aug 8, 12:45 - 13:45 PDT

Where: Red Team VIg

SpeakerBio:Jonathan Helmus

Jonathan Helmus - Security engineer and educator who has been working in engineering, security, and information technology for 10 years. Specializations in Penetration Testing, Threat and Adversarial Assessments, Vulnerability Management, Cloud Technology (AWS), and experience as a Technical Educator and University Level Professor.

Description:

This presentation will go through various steps on how students can bridge the gap between academia and becoming a penetration tester. This will include a breakdown of certifications to get, career fields to take on before getting in the industry, what to expect, and speed bumps and road blocks that students can expect to see in their journey.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

Return to Index - Add to  - ics [Calendar](#) file

Title: The Underestimated Threat Vector: Homogeneity

When: Sunday, Aug 9, 13:15 - 13:45 PDT

Where: BioHacking Vlg

SpeakerBio: Vidya Murthy , Vice President Operations, MedCrypt

Vidya is fascinated by the impact of cybersecurity on the healthcare space. Beginning her career in consulting, she realized a passion for healthcare and worked for global medical device manufacturer Becton Dickinson. She has since joined MedCrypt, a company focused on bringing cybersecurity leading practices to medical device manufacturers. Vidya holds an MBA from the Wharton School.

Description:

The number of times I've heard it's a pipeline issue and there just aren't enough candidates enrages me. And yet when I finally have the ability and breath to actually make change, I'm struggling to find candidates. What am I doing wrong? And if with all my intent I'm still struggling, what hope is there for the industry? This talk explores why the burden of dismantling systemic racism in cybersecurity requires practitioners of every race, sector, and discipline.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Vulnerability That Gmail Overlooked and Enabling Threat Hunting

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Packet Hacking Vlg - Talk

SpeakerBio:Özkan Mustafa Akkus , Vulnerability Researcher and Penetration Testing Expert, Barikat Cyber Security Ozkan (Twitter: @ehakkus) is a vulnerability researcher and penetration testing expert in Turkey. While studying sports sciences and technologies, he decided to leave the University and step into the world of Cyber Security. His purpose is to provide added value to the world of cyber security through the training he has given and the research he has conducted. Ozkan publish security vulnerabilities on international platforms that he has discovered. He shares his experiences and works on his personal blog <https://www.pentest.com.tr>. Ozkan also has many internationally recognized certificates such as OSWE, OSCE, OSCP, OSWP, CEH, CCNA, TSE-STU. He gave trainings and presentations in many universities and institutions in his country. In addition to these studies, He gave the presentation of "0day Hunting and RCE Exploitation in Web Applications" in AppSec Village at Defcon 27.

Twitter: [@ehakkus](https://twitter.com/ehakkus)

Description:

The use and working logic of the SMTP protocol is very simple, but it poses different threats. Large e-mail infrastructures such as Gmail can forget important and critical points that may threaten the security of people while using this protocol. By explaining this primitive structure of the SMTP protocol, we will examine the vulnerability that I discovered in Gmail. We will also do live examples.

YouTube: <http://youtube.com/wallofsheep>

Twitch: <http://twitch.tv/wallofsheep>

Facebook: <http://facebook.com/wallofsheep/>

Periscope: <https://t.co/gnl7JLftA?amp=1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: The Worst Mobile Apps

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: Packet Hacking VIg - Talk

SpeakerBio: Sam Bowne , Founder, Infosec Decoded Inc.; Instructor, 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

Twitter: [@sambowne](https://twitter.com/sambowne)

Description:

I've audited hundreds of Android apps and now, thanks to the Checkra1n jailbreak, iOS apps as well. Many of these apps have security flaws such as exposing passwords on the phone or in network traffic, but a few of them are spectacularly insecure, exposing the entire user database to every user. I will explain how to perform simple tests to detect such errors and demonstrate them with live apps on both Android and iOS devices. Don't let this happen to your app!

YouTube: <http://youtube.com/wallofsheep>

Twitch: <http://twitch.tv/wallofsheep>

Facebook: <http://facebook.com/wallofsheep/>

Periscope: <https://t.co/gnl7JLlftA?amp=1>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Friday - 13:00-13:59 PDT

Title: This year's village badge

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Monero Vlg

SpeakerBio: Michael Schloh von Bennewitz

No BIO available

Description:

Codenamed Bob, this year's electronic badge enjoys collaboration from several villages and is called the Intervillage Badge. <https://bob.monerodevices.com/> In this hour, we review the construction and feature set of this unique electronic badge. We consider it's energy harvesting ability, hackable nature, and radio signature. This year's badge contains three RFID/NFC long range circuits, dome switches never seen before on badges, and a trapazoidal 13.56 MHz trace antenna. It is enclosed in a translucent colored plastic frame, a full colour front overlay, and back mounted color leatherette (to protect your phone lens.) The Opensource design is located on scm.monerodevices.com with several of your Monero friends participating in the project. The Intervillage Badge is distributed by well known sellers, please see shop.monerodevices.com for information. For more information about this year's village badge (and many others), please visit the Monero Village office hours. View the schedule at Monerovillage.org and look for 'Badge Clinic'.

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

Return to Index - Add to  - ics [Calendar](#) file

Title: Threagile - Agile Threat Modeling with Open-Source Tools from within Your IDE

When: Sunday, Aug 9, 09:00 - 09:45 PDT

Where: AppSec Vlg

SpeakerBio:Christian Schneider

No BIO available

Twitter: [@cschneider4711](https://twitter.com/cschneider4711)

Description:

The open-source tool Threagile enables agile teams to create a threat model directly from within the IDE using a declarative approach: Given information about the data assets, technical assets, communication links, and trust boundaries as input in a simple to maintain YAML file, it executes a set of over 40 built-in risk rules, which can be extended with custom risk rules, against the processed model. The resulting artifacts are graphical diagrams, Excel, and PDF reports about the identified risks, their rating, and the mitigation steps as well as risk tracking state. DevSecOps pipelines can be enriched with Threagile as well to process the JSON output.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Threat Hunting with the Elastic Stack (Beginner)

When: Friday, Aug 7, 15:00 - 16:30 PDT

Where: Blue Team VIg - Workshop Track 2

SpeakerBio: Ben Hughes

Ben Hughes (@CyberPraesidium) brings over 15 years of diverse experience in cyber security, IT, and law. He leads Polito's commercial services including pen testing, DFIR, and threat hunting. Prior to joining Polito, Ben worked on APT hunt teams at federal and commercial clients. He holds CISSP, GWAPT, and GCFA certifications.

Twitter: @CyberPraesidium

Description:

This hands-on workshop will walk you through leveraging the open source Elastic (ELK) stack to proactively identify attacker activity hiding within diverse data sets. The basic tools and techniques taught during this workshop can be used to investigate isolated security incidents or implemented at scale for continuous monitoring and threat hunting. You will be provided with access to a preconfigured Elastic cluster and extensive sample logs containing malicious endpoint and network events waiting to be discovered on a simulated enterprise network. Emphasis will be placed on live demos and practical training exercises throughout.

With all new logs and revamped material from our past versions of this workshop, this year's hands-on workshop will walk attendees through leveraging the open source Elastic (ELK) stack to proactively identify malicious activity hiding within diverse data sets. The basic tools and techniques taught during this class can be used to investigate isolated security incidents or implemented at scale for continuous monitoring and threat hunting. Attendees will be provided with access to a preconfigured Elastic cluster and extensive sample logs containing malicious endpoint and network events waiting to be discovered on a simulated enterprise network. New for this year, attacker artifacts will be more closely mapped to the MITRE ATT&CK Framework and tagged accordingly in the provided logs to help demonstrate the value of log enrichment, showcase both common and novel real-world attacker TTPs, and leverage a methodological approach to adversary and anomaly detection. Emphasis will be placed on live demos and practical training exercises throughout.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Threat Modelling the Death Star

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: AppSec Vlg

SpeakerBio: Mário Areias

No BIO available

Description:

It is a known fact the Empire needs to up their security game. The Rebellion hack their ships, steal their plans, and even create backdoors! In this talk, we will help the Empire by threat modeling the Death Star. Traditionally, Threat Models have been a slow and boring process that ends up with a giant document detailed any possible security problem. This approach, although useful in the past, is not necessarily good in an ever-changing environment (or when you have Jedis as enemies!).

I will introduce Attack Trees and how they can fit in nicely in a DevOps world. Come and join the Dark Side! We might save the Empire after all!

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Ticketing To Takeoff: An Airport Hacking Choose Your Own Adventure

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Aerospace VIg

SpeakerBio:Liz Wharton

Liz, a technology-focused business and public policy attorney, has advised researchers, startups, and policymakers at the federal, state, and local level. Currently SCYTHE's Chief of Staff, she was the World's Busiest Airport's technology attorney and hosted the Buzz Off with Lawyer Liz podcast.

Description:

Check-in software glitches, payment system data breaches, gate signage ransomware attacks... Airports are an interconnected, mini-smart city of retail, dining, infrastructure, and transportation logistics operated by a hodgepodge of business interests + federal, state, and local entities and agencies. Join an interactive adventure as a passenger navigating the airport to catch a flight before hackers cause chaos, highlighting security pitfalls and risks all based on publicly disclosed incidents.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Total E(A)gression

When: Friday, Aug 7, 18:00 - 18:59 PDT

Where: Red Team VIg

SpeakerBio: Alvaro Folgado Rueda

Rebujacker works as a Product Security Engineer at Salesforce. He has multiple years of experience performing penetration tests, security assessment against different technologies, building automation tools for this purpose and performing application level research. In the recent years his field of study has been focused into red teaming and automation. The combination of his application level security and pentesting knowledge leads him to build tools/implants that blends-in better with nowadays cloud infrastructure and application stack of tested organizations. Working recently in its main project: Siesta Time Implant Framework for red teamers, presented in last Defcon Red team Village. Last progress includes new persistence and stealthier network modules.

Description:

Defensive techniques and tools keep getting better and therefore the creation of implants that are not detected is a harder and time consuming task every Red Team operator has to go through. Focusing on the network detection field; recent Intrusion Detection Systems (IDS) that uses new network analysis techniques can detect easily some of our handcrafted implants by analyzing connection fingerprints from both client and server side. In some environments, techniques like Deep Packet Inspection can map our implants to possible threats to be addressed. In this talk, I provide solutions that can be used on implants; a modified TLS Go package that allows circumventing tools like JA3 by providing desired fingerprints that will help to mimic rightful client software, egression to Gmail servers and techniques like steganography/encryption to hide obvious payloads. All these ideas are tailored into a new network modules for the Siesta Time Framework, to help to automate the creation of desired Implants. As a finale, possible new defensive techniques to improve tools like JA3 will be explained.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Towards an Institutional Review Board for Biohackers

When: Saturday, Aug 8, 14:45 - 15:15 PDT

Where: BioHacking Vlg

SpeakerBio:Dr. Sarah Blossom Ware

Dr. Sarah Blossom Ware is Founder of BioBlaze Community Bio Lab in West Chicago, Illinois. She also teaches biology, humanities and writing at the university level. Sarah strives to bridge gaps between traditional scientists/members of regulatory agencies and non-traditional scientists/biohackers.

Description:

Institutional Review Boards (IRBs) are groups that examine research plans of fellow members by applying community standards to that research. IRBs help researchers consider rigorous methodology, ethics and safety and the protection of vulnerable populations of people or animals. IRB approval is required by the FDA before human clinical trials can begin. People who serve on IRBs include general community members, researchers, bioethicists, physicians, clinicians, lawyers and members of regulatory agencies. Traditional research corporations and universities have internal IRBs, but external independent IRBs do also already exist. However, it is usually very expensive to hire an independent IRB, so most non-traditional scientists cannot afford it. This creates a major hindrance to bringing innovative human health related solutions to the general public. There has recently been a small grassroots push in the biohacking community to try to create an independent IRB for the biohacking community to help bridge this gap.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Tracer FIRE 9 (Intermediate)

When: Saturday, Aug 8, 12:00 - 13:30 PDT

Where: Blue Team Vlg - Workshop Track 1

SpeakerBio: Andrew Chu

I am a senior undergraduate student working towards a B.S. in Computer Science at Purdue University. I've also worked as a year round R&D intern at Sandia National Laboratories for ~6 years, doing work on topics such as web exploitation, network virtualization, and malware classification.

Description:

Tracer FIRE 9 (Forensic Incident Response Exercise) is a team-oriented, CTF-style exercise in which participants develop forensic incident response skills through a virtual simulated environment. It aims to provide a target rich setting for practicing forensic techniques, and utilizes malware from real-world APT campaigns to bridge the gap between reality, and a synthetic task context. At the end of the exercise, participants will have had the chance to interact with various forensic tools and files widely encountered in actual Blue Team operations, and will additionally be exposed to invaluable reflection on potential attack matrices used in exploitation.

Tracer FIRE (Forensic Incident Response Exercise) is a combined simulation and live exercise program developed by Sandia National Laboratories to help cyber security incident responders, analysts, and operators become proficient in critical skill areas. These exercises simulate various events such as attacks, emergencies, and disruptions to critical infrastructure. Participants in this latest Tracer FIRE scenario are hired by the electric skateboard company, WheelByte, to investigate a series of cyber attacks resulting in exfiltration of company data, degradation of service, and damage to consumer confidence. Provided with a set of artifacts spanning raw email sessions, network packet captures, disk images, and memory images, participants conduct analysis to advance their investigation. Tools such as Security Onion and Ghidra are then used to parse said artifacts, yielding intriguing findings which may then be merged for development of an overarching view of the scenario. Through such means, participants can gain understanding of potential approaches for emerging cybersecurity issues.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Trends in the online card payment security

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Payment Vlg

SpeakerBio:Dr Mohammed Aamir Ali

Mohammed (Mo) Ali is currently the global head for digital development GCO at Boehringer Ingelheim Pharmaceuticals. Prior to this role he served as a Director within the R&D Operations and Innovations group at J&J Pharmaceuticals and also as one of the first founding members of the digital development group and Strategic Program Office at Novartis, responsible for several "E" initiatives within Digital Health. These programs aim to serve the needs of patients by creating a digital footprint and platform which would assist in the overall delivery and enrichment of their experience.

Description:

Ever since the world-wide web emerged in the early nineties we have seen dramatic changes in how we pay, including the proliferation of online card payments, the introduction of mobile and contactless payment as well as the rise of bitcoin. Security is a key concern in the design and use of these payment methods, but these cannot be understood without also considering legacy issues, usability concerns and business incentives.

In this talk, I will start from the fundamentals of the online card payment system, its types and will also expand on the security features of each type. I'll then discuss the inherent vulnerabilities of the system, the competing incentives of the many parties that are involved in payment and the role of PCI DSS and other approaches to resolve security challenges. This talk exposes attendees to the relevant industrial standards and approaches, introduces some cutting-edge research outcomes, and provides insight in the many competing concerns that impact on the online card payment security.

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Saturday - 16:00-16:30 PDT

Title: Tricky Bundles: Smarter Dependency Management for I2P-Bundling Applications

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: Monero Vlg

SpeakerBio: idk

No BIO available

Description:

We will explore the use of I2P distributions like Monero's own i2p-zero and how they can be used to create and distribute I2P applications that use I2P for networking in non-JVM languages, best practices for creating a tricky bundle, and how tricky bundles can help bridge the gaps between I2P and the applications that it can adapt. As part of this, we will examine the structure of I2P from a non-I2P developer's perspective, and explore it's relationships to the applications that use it with examples from the Java distribution and with third-party applications that use SAM.

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/70820826769945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Trust And Truth In Space Situational Awareness

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: Aerospace VIg

SpeakerBio: James Pavur , DPhil Student, Oxford University

James Pavur is a Rhodes Scholar at Oxford University working on a DPhil in Cyber Security. His academic research is primarily on the threats to satellite systems with a focus on satellite communications and trustworthy spaceflight operations. Prior to Oxford, he majored in Science, Technology and International Affairs (STIA) at Georgetown University where he graduated with the School of Foreign Service Dean's Medal (highest cumulative GPA) in 2017.

He has held numerous internships and professional positions related to information security. This included acting as Director of Information Security for Students of Georgetown Inc. (The Corp), a student run non-profit with more than 300 employees. He has also assisted with computer crimes investigations as an intern with the United States Postal Service Office of the Inspector General, worked on embedded systems reverse-engineering as an intern at Booz Allen Hamilton, and even pentested air-conditioners for the Public Buildings Services while working for Telos Corporation.

Outside of computers, James enjoys flying kites and collecting rare and interesting teas.

Twitter: [@JamesPavur](https://twitter.com/JamesPavur)

Description:

Space Situational Awareness Data (SSA) is the lifeblood of responsible spaceflight. With tens of thousands of debris objects in orbit, knowing where and when collisions may occur is key to preventing lasting environmental harm. However, SSA data collection is inordinately complex, creating natural incentives for centralized information sharing. When actors lack the capability to independently monitor the state of orbit, they find themselves forced to trust third parties.

In this talk, we consider how a sufficiently motivated attacker might modify SSA repositories to deliberately conceal or falsify collision projections to influence the behaviors of satellite owners. In addition to a high-level discussion of the relevant threat model, we will present simulated implementations of these attacks. We will also briefly consider various mitigation techniques which can be employed by both SSA operators and data recipients against such attacks.

This talk will touch on basic principles of orbital dynamics and spaceflight operations but assumes no prior background in physics. It is intended to serve as starting point for those interested in how the physical dynamics of outer space can manifest as unique security challenges.

This event will be coordinated on the DEF CON Discord server, in channel #av-space-text.

Discord: <https://discord.com/channels/708208267699945503/732394328105943180>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Trust, but Verify: Maintaining Democracy In Spite of

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: Red Team VIg

SpeakerBio:Allie Mellen

Allie Mellen - I've spent several years in cybersecurity and have been recognized globally for my security research. Over the past year, I have helped organize and execute multiple election security tabletop exercises with participants from the FBI, Secret Service, Department of Homeland Security, and state law enforcement. In these sessions, it's hackers versus law enforcement as an exercise in what attackers can do to disrupt Election Day and what the government is prepared to do - or should be prepared to do - to stop them.

Description:

In this session, we'll discuss how Russia has influenced worldwide elections using cyberwarfare and how countries have fought back. We'll understand the natural asymmetry between how countries are able to respond, and how they have changed their approach since 2016.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Turning Telemetry and Artifacts Into Information (Intermediate)

When: Friday, Aug 7, 13:30 - 14:59 PDT

Where: Blue Team Vlg - Workshop Track 1

SpeakerBio: Omenscan

No BIO available

Description:

There are many excellent FOSS triage and live response tools for Windows. They can dive deep into Windows systems to extract the artifacts and telemetry that might identify what happened on a machine.

However, after extracting those artifacts, it is usually up to the analyst to parse and reformat the raw data from these artifacts to make sense of them.

What if you are looking for a basic, repeatable, automated way to create an overview of what happened on a machine? In this Show And Tell we'll walk through the process of turning raw artifacts into useful information.

The presenter has spent many years developing tools and methods to help junior forensic analysts collect, parse, and make sense of Windows telemetry and artifacts. And in the process help them learn more.

In this Show And Tell, we will walk through the process of doing an automated, targeted collection on a suspicious machine. We will take that collection, and use Open Source tools to turn that data into an immediately useful report. We will also cover how to collect locally, and remotely - and the unique challenges that each presents.

We will start with collecting data from a suspicious endpoint using AChoir, and creating a report from that data using AChReport. We will also use tools like Volatility and Loki to automate memory analysis and determine if something malicious is located in memory. We will cover this process for both live systems, and collected memory dumps. And we will talk about when you would use one method over the other.

Finally, we will take the collected data, and show how to run Plaso against it to get a timeline which can be further processed for a more detailed analysis.

This workshop is relevant for both the novice and experienced forensic analyst. It is targeted at automating parts of the forensic analysis process to find common signs of malicious activity. We will use specific tools, but the goal is to show how forensic tools can be automated to enhance the forensic analysis process.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Twitter Word Phrency

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: Recon VIg

SpeakerBio:Master Chen

No BIO available

Description:

What you say can hurt you, but how? In this talk, I will take a deep dive into Twitter Word Phrency analysis and the implications of the resulting data. I will cover data acquisition, curation, analysis, weaponization, and maybe even profit. What is revealed by everyday social media engagemt? Predictive speech? Password lists? Automated trolling? Let's find out!

Recon Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/c/ReconVillage>

#rv-talks-text: <https://discord.com/channels/708208267699945503/737048009732522014>

Return to Index - Add to  - ics [Calendar](#) file

BCV - Saturday - 10:10-10:59 PDT

Title: Twitter's Tax Day Disaster: The Beginning (and End) of Mainstream Crypto Scams

When: Saturday, Aug 8, 10:10 - 10:59 PDT

Where: Blockchain VIg

SpeakerBio: Victor Fang

No BIO available

Description: No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ETV - Friday - 12:00-12:59 PDT

Title: U.S. Privacy and Civil Liberties Oversight Board Member

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: Ethics VIg

SpeakerBio: Travis LeBlanc

No BIO available

Description:

This will be a pre-recorded talk.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: ULTIMATE Secure Coding Throwdown (Secure Code Warrior)

When: Friday, Aug 7, 09:00 - 23:59 PDT

Where: See Description or Village

Description:

Are. You. Ready? Head to the AppSec battlefield and prove that you are the ultimate secure coding champion. Go head-to-head with your peers as you test your web application security knowledge of the OWASP Top 10. Strut your skills. Crush the competition. Score excellent prizes and take home the title of Secure Code Warrior!

Players will be presented with a series of vulnerable code challenges that will ask them to identify the problem, locate the insecure code, and fix the vulnerability. Select from a range of software languages to complete the tournament, including Java EE, Java Spring, C MVC, C WebForms, Ruby on Rails, Python Django, Scala Play & Node.JS. It's gamified, it's relevant, but most of all - it's fun.

Watch as you earn points and climb to the top of the real-time leaderboard during the event. Prizes will be awarded to the top 3 point scorers, with one security superhero being crowned the ultimate Secure Code Warrior. Will it be you?

Psst: Want to test your secure coding skills at your own pace, without the competition? You're welcome to come along and join the fun

Web: <https://discover.securecodewarrior.com/DEFCON28-tournament.html>

Forum: <https://forum.defcon.org/node/232898>

Discord: <https://discord.com/channels/708208267699945503/741327638815309984>

Return to Index - Add to  - ics [Calendar](#) file

Title: ULTIMATE Secure Coding Throwdown (Secure Code Warrior)

When: Saturday, Aug 8, 00:00 - 23:59 PDT

Where: See Description or Village

Description:

Are. You. Ready? Head to the AppSec battlefield and prove that you are the ultimate secure coding champion. Go head-to-head with your peers as you test your web application security knowledge of the OWASP Top 10. Strut your skills. Crush the competition. Score excellent prizes and take home the title of Secure Code Warrior!

Players will be presented with a series of vulnerable code challenges that will ask them to identify the problem, locate the insecure code, and fix the vulnerability. Select from a range of software languages to complete the tournament, including Java EE, Java Spring, C MVC, C WebForms, Ruby on Rails, Python Django, Scala Play & Node.JS. It's gamified, it's relevant, but most of all - it's fun.

Watch as you earn points and climb to the top of the real-time leaderboard during the event. Prizes will be awarded to the top 3 point scorers, with one security superhero being crowned the ultimate Secure Code Warrior. Will it be you?

Psst: Want to test your secure coding skills at your own pace, without the competition? You're welcome to come along and join the fun

Web: <https://discover.securecodewarrior.com/DEFCON28-tournament.html>

Forum: <https://forum.defcon.org/node/232898>

Discord: <https://discord.com/channels/708208267699945503/741327638815309984>

Return to Index - Add to  - ics [Calendar](#) file

Title: ULTIMATE Secure Coding Throwdown (Secure Code Warrior)

When: Sunday, Aug 9, 00:00 - 15:59 PDT

Where: See Description or Village

Description:

Are. You. Ready? Head to the AppSec battlefield and prove that you are the ultimate secure coding champion. Go head-to-head with your peers as you test your web application security knowledge of the OWASP Top 10. Strut your skills. Crush the competition. Score excellent prizes and take home the title of Secure Code Warrior!

Players will be presented with a series of vulnerable code challenges that will ask them to identify the problem, locate the insecure code, and fix the vulnerability. Select from a range of software languages to complete the tournament, including Java EE, Java Spring, C MVC, C WebForms, Ruby on Rails, Python Django, Scala Play & Node.JS. It's gamified, it's relevant, but most of all - it's fun.

Watch as you earn points and climb to the top of the real-time leaderboard during the event. Prizes will be awarded to the top 3 point scorers, with one security superhero being crowned the ultimate Secure Code Warrior. Will it be you?

Psst: Want to test your secure coding skills at your own pace, without the competition? You're welcome to come along and join the fun

Web: <https://discover.securecodewarrior.com/DEFCON28-tournament.html>

Forum: <https://forum.defcon.org/node/232898>

Discord: <https://discord.com/channels/708208267699945503/741327638815309984>

Return to Index - Add to  - ics [Calendar](#) file

Title: Understanding Cyber-Attacks and Their Implications to Democratic Regimes

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: Voting Vlg

SpeakerBio:Javier F. Patiño García , MPP Candidate, University of Chicago Harris School of Public Policy
No BIO available

Description:

Cyber-security experts have documented how authoritarian regimes attacked the US voting infrastructure or how this type of governments stole information from American companies. This evidence suggests that authoritarian regimes are more likely to conduct cyber-attacks than democratic ones. The purpose of this research is to prove this hypothesis. With information from the Center for Strategic and International Studies (CSIS), this research provides a descriptive analysis of the Significant Cyber Incidents that occurred worldwide from 2006 to 2019. To prove the former hypothesis, this research shows the results from panel data models with random and fixed effects, which provide evidence that confirms this hypothesis: authoritarian regimes are more likely to commit cyber-attacks than democratic states. However, there is no evidence to sustain that democracies are more likely to be attacked than authoritarian regimes. In otherwords, all regimes are subject to cyber-attacks.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Understanding Space Through a CyberSecurity Lens

When: Friday, Aug 7, 10:00 - 13:30 PDT

Where: Aerospace VIg Workshop

Description:

This exciting, fast-paced course delivers the "big picture" of space missions from cradle to grave. Understanding Space is the ideal course for technical or non-technical professionals new to the space industry or who need a refresher on the fundamentals.

Learning outcomes will be:

- Gain Core Space Knowledge
- Comprehend space mission Capabilities, Trade-offs and Limitations - Apply Space Concepts to real-world problems - Analyze Typical Space Problems
- Synthesize concepts to Design a Space Mission - Evaluate basic technical and programmatic space issues

This will be a half-day course instead of the normal 2-day course.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Understanding Space Through a CyberSecurity Lens

When: Friday, Aug 7, 14:30 - 17:59 PDT

Where: Aerospace VIg Workshop

Description:

This exciting, fast-paced course delivers the "big picture" of space missions from cradle to grave. Understanding Space is the ideal course for technical or non-technical professionals new to the space industry or who need a refresher on the fundamentals.

Learning outcomes will be:

- Gain Core Space Knowledge
- Comprehend space mission Capabilities, Trade-offs and Limitations - Apply Space Concepts to real-world problems - Analyze Typical Space Problems
- Synthesize concepts to Design a Space Mission - Evaluate basic technical and programmatic space issues

This will be a half-day course instead of the normal 2-day course.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Understanding Space Through a CyberSecurity Lens

When: Saturday, Aug 8, 09:00 - 12:30 PDT

Where: Aerospace VIg Workshop

Description:

This exciting, fast-paced course delivers the "big picture" of space missions from cradle to grave. Understanding Space is the ideal course for technical or non-technical professionals new to the space industry or who need a refresher on the fundamentals.

Learning outcomes will be:

- Gain Core Space Knowledge
- Comprehend space mission Capabilities, Trade-offs and Limitations - Apply Space Concepts to real-world problems - Analyze Typical Space Problems
- Synthesize concepts to Design a Space Mission - Evaluate basic technical and programmatic space issues

This will be a half-day course instead of the normal 2-day course.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Understanding Space Through a CyberSecurity Lens

When: Saturday, Aug 8, 13:30 - 16:59 PDT

Where: Aerospace VIg Workshop

Description:

This exciting, fast-paced course delivers the "big picture" of space missions from cradle to grave. Understanding Space is the ideal course for technical or non-technical professionals new to the space industry or who need a refresher on the fundamentals.

Learning outcomes will be:

- Gain Core Space Knowledge
- Comprehend space mission Capabilities, Trade-offs and Limitations - Apply Space Concepts to real-world problems - Analyze Typical Space Problems
- Synthesize concepts to Design a Space Mission - Evaluate basic technical and programmatic space issues

This will be a half-day course instead of the normal 2-day course.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Understanding Space Through a CyberSecurity Lens

When: Sunday, Aug 9, 09:00 - 12:30 PDT

Where: Aerospace VIg Workshop

Description:

This exciting, fast-paced course delivers the "big picture" of space missions from cradle to grave. Understanding Space is the ideal course for technical or non-technical professionals new to the space industry or who need a refresher on the fundamentals.

Learning outcomes will be:

- Gain Core Space Knowledge
- Comprehend space mission Capabilities, Trade-offs and Limitations - Apply Space Concepts to real-world problems - Analyze Typical Space Problems
- Synthesize concepts to Design a Space Mission - Evaluate basic technical and programmatic space issues

This will be a half-day course instead of the normal 2-day course.

[Return to Index](#) - Add to  - ics [Calendar](#) file

DCG - Saturday - 14:00-14:59 PDT

Title: Understanding the Threat: Malicious Software, Malicious Actors, and the Promise of Connected Medical Technology

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: DEF CON Groups

Description:

Presentation by DC858 (San Diego, California, USA)

All DEF CON Groups presentations are happening in AltSpace.

AltSpace: <https://account.altvr.com/events/1520704529866162594>

Listen @ #dcg-stage-voice: <https://discord.com/channels/708208267699945503/740428852999880704>

Interact @ #dcg-stage-text: <https://discord.com/channels/708208267699945503/710379858429083698>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Velociraptor: An Introduction Into OpenSOC CTF Tools

When: Thursday, Aug 6, 14:15 - 14:59 PDT

Where: Blue Team VIg - Workshop Track 1

SpeakerBio: Mike Cohen

Mike is a digital forensic researcher and senior software engineer. He's supported leading open-source DFIR projects including as a core developer of Volatility and lead developer of both Rekall and Grr Rapid Response while working for the Google IR team. Mike founded Velocidex in 2018 - the company behind Velociraptor. Mike is our "Digital Paleontologist" and brings his years of expertise to the role of principal developer of Velociraptor.

Twitter: [@velocidex](#)

Description:

Learn. Play. Do

We then demonstrate some of the major features that you can use to rapidly investigate, triage and contain adversaries on your network.

Try Velociraptor by downloading it from Github at <https://github.com/Velocidex/velociraptor>

Every year the Blue Team Village hosts OpenSOC. A unique defense CTF meant to teach and test practical incident response skills in an environment that's as close to "the real thing" as it gets.

This year BTV wanted to do more. We know that some Blue Teamers might be unfamiliar with some of the tools used by OpenSOC. And we didn't want that to keep anyone from playing this incredible defense simulation.

So this year we are dedicating all day Thursday to demo the various OpenSOC tools, before OpenSOC starts on Friday. These are tools like Graylog, Moloch, Zeek, Osquery, and others that Blue Teamers rely on every day to defend their networks against attackers.

That means that after you LEARN the tools, you can PLAY the OpenSOC CTF, and then take that knowledge back to your own Blue Team to DO the work of defending your network.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

BCV - Friday - 11:00-11:59 PDT

Title: Verifiable Delay Functions for preventing DDoS Attacks on Ethereum 2.0

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Blockchain Vlg

Speakers:Gokul Alex,Tejaswa Rastogi

SpeakerBio:Gokul Alex

No BIO available

SpeakerBio:Tejaswa Rastogi

No BIO available

Description:No Description available

Blockchain Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/blockchainvillage>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Veteran Transition Tips

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: Career Hacking Vlg

SpeakerBio:Bob Wheeler

No BIO available

Description:

There's no shortage of advice out there for transitioning veteran job seekers – unfortunately much of the advice tends to be cookie cutter tips focusing on the most basic of topics. This program will help transitioning veterans in the cyber security industry understand the hiring landscape, highlight the difference between the recruiters who put you in the service and ones working to help you land that first job as a civilian, as well as how to leverage job board and job fairs, including virtual events. We'll even put some special emphasis on how to really build your professional network and manage a your transition from different geographical locations.

Career Hacking Village activities can be watched on YouTube.

CHV YouTube: https://www.youtube.com/channel/UCxF_PpndJEoi4fsrQx6yuQw

[Return to Index](#) - Add to  - ics [Calendar](#) file

HRV - Sunday - 14:30-14:45 PDT

Title: Village Closing Commentary

When: Sunday, Aug 9, 14:30 - 14:45 PDT

Where: Ham Radio Vlg

Description:

As our village wraps up for this year, a huge thank you to everyone for participating!

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar file](#)

HRV - Friday - 10:00-10:15 PDT

Title: Village Opening Remarks

When: Friday, Aug 7, 10:00 - 10:15 PDT

Where: Ham Radio Vlg

Description:

Welcome to Ham Radio Village @ DEF CON Safe Mode

This Ham Radio Village event will be held on Twitch. Related conversation will be held in the DEF CON Discord, channel #ham-presentation-text (Q&A).

Twitch: <https://www.twitch.tv/hamradiovillage>

#ham-presentation-text: <https://discord.com/channels/708208267699945503/736674835413073991>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Violent Python 3

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: Packet Hacking Vlg - Workshop

Speakers:Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handleman,Sam Bowne

SpeakerBio:Elizabeth Biddlecome , Part-time Instructor, City College San Francisco

Elizabeth Biddlecome is a consultant and instructor, delivering technical training and mentorship to students and professionals. She is a senior instructor for Infosec Decoded, Inc. 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

Irvin Lemus has served clients throughout California, providing valuable professional services that bring peace of mind to clients as well as security against the constant threats with our ever-connected world.

SpeakerBio:Kaitlyn Handleman

Kaitlyn Handleman is a Professional Red Teamer.

SpeakerBio:Sam Bowne , Founder, Infosec Decoded Inc.; Instructor, 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

Twitter: [@sambowne](https://twitter.com/sambowne)

Description:

Even if you have never programmed before, you can quickly and easily learn how to make custom hacking tools in Python. We build tools that perform port scanning, brute-force attacks, crack password hashes, and XOR encryption. Python is among the top three programming languages in the world, for good reason: it's the easiest language to use for general purposes.

This workshop requires registration. If you are registered, please proceed to #phv-infobooth-text and you'll be given access to join.

#phv-infobooth-text: <https://discord.com/channels/708208267699945503/708242376883306526>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Saturday - 12:15-13:15 PDT

Title: Vivisecting PowerPC

When: Saturday, Aug 8, 12:15 - 13:15 PDT

Where: ICS V1g

Speakers:ac0rn,atlas Of d00m

SpeakerBio:ac0rn

No BIO available

SpeakerBio:atlas Of d00m

No BIO available

Description:No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Vote @ Home Workshop

When: Saturday, Aug 8, 12:00 - 14:10 PDT

Where: Ethics VIg

SpeakerBio: Andrea Matwyshyn

No BIO available

Description:

This will be a 40-minute pre-recorded talk, followed by a 30-minute live Q&A session.

Twitch: <https://www.twitch.tv/ethicsvillage>

#ev-talks-voice: <https://discord.com/channels/708208267699945503/730299696454696980>

#ev-general-text: <https://discord.com/channels/708208267699945503/732732980342030449>

[Return to Index](#) - Add to  - ics [Calendar file](#)

Title: Vote-from-home? Review of Election Security on Remote Voting in Response to COVID-19

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: Voting Vlg

SpeakerBio: Sang-Oun Lee , Applied Data Fellow, International Innovation Corps, University of Chicago
No BIO available

Description:

This presentation poses a question on whether the remote voting by online or vote-by-mail is trustworthy under the COVID-19 pandemic situation. One of the worldwide efforts to contain the virus was to work-from-home and restriction orders. Besides, because of the human contact is critical in the dissemination of the virus, possibilities of alternative methods of voting such as online voting, blockchain voting, vote-by-mail are proposed. In light of such a situation, the article proposes a framework to evaluate the election security of remote voting methods. Further, the article provides a case of best practice for election administration from the case of the Republic of Korea. Based off of the assessment results from the proposed evaluation framework, the article provides modest suggestions and policy implications to the election administrators.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ICS - Friday - 11:45-12:15 PDT

Title: Vulnerability Discovery - Tips for Surviving and Thriving

When: Friday, Aug 7, 11:45 - 12:15 PDT

Where: ICS Vlg

Speakers: Dor Yardeni, Mike Lemley

SpeakerBio: Dor Yardeni

No BIO available

SpeakerBio: Mike Lemley

No BIO available

Description: No Description available

ICS Village activities will be streamed to YouTube and Twitch.

YouTube: https://www.youtube.com/channel/UCL_GT2-OMrsqqglv0JijHhw

Twitch: https://www.twitch.tv/ics_village

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Saturday - 10:00-10:30 PDT

Title: War By Other Means: How Influence Operations Undermine Democracy

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: Voting Vlg

SpeakerBio: Ben Dubow , CTO and President, Omelas

No BIO available

Description:

New tactics and capabilities in information warfare give authoritarians unprecedented power to "hack" the electorates. Our research on campaigns in Poland and Taiwan show the breadth and impact of operations against democracies around the world and what they foreshadow for the US Presidential election.

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: War Story Bunker

When: Friday, Aug 7, 18:00 - 19:59 PDT

Where: See Description or Village

Description:

One of our favorite parts of DEF CON every year is hearing about what other hackers have been up with harrowing tales of red team exercises gone wrong, or so very right. We've also heard of valiant efforts of defense from our blue team folks while waiting in Linecon. Do you have a cool "war story" to share? Would you like to listen to some fun stories from your fellow hackers? This is the place to be. Join the DEF CON CFP Board, Goons, and fellow hackers around the bunker.

Selected speakers will get 15 minutes to tell their stories on the Discord voice channel, and audience members will be able to ask questions, or discuss on the text channel.

The sign up form won't be open until the night of the event, participation will be first come first serve, and subject to moderation.

Discord: <https://discordapp.com/channels/708208267699945503/733562251285495818/736711109037522944>

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Saturday - 22:45-23:59 PDT

Title: Weaponized XSS - Moving Beyond Alert(1)

When: Saturday, Aug 8, 22:45 - 23:59 PDT

Where: Red Team VIg

SpeakerBio:Ray Doyle

No BIO available

Description:No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Web Shell Hunting - Part 1

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: AppSec Vlg

SpeakerBio: Joe Schottman

No BIO available

Twitter: [@JoeSchottman](#)

Description:

Web shells 101.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8Ll0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

ASV - Saturday - 12:00-13:59 PDT

Title: Web Shell Hunting - Part 2

When: Saturday, Aug 8, 12:00 - 13:59 PDT

Where: AppSec Vlg

SpeakerBio: Joe Schottman

No BIO available

Twitter: [@JoeSchottman](#)

Description:

Web shells are malicious web applications used for remote access to and control of compromised servers. This workshop covers methods to detect web shells at the system and network level.

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

VMV - Friday - 10:00-10:30 PDT

Title: Welcome and Kick-Off

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: Voting Vlg

Speakers:Harri Hursti,Matt Blaze,Maggie MacAlpine

SpeakerBio:Harri Hursti

Co-Founder, DEF CON Voting Village

Founding Partner, Nordic Innovation Labs

SpeakerBio:Matt Blaze

Co-Founder, DEF CON Voting Village

Professor of Law and McDevitt Chair for the Department of Computer Science, Georgetown University

SpeakerBio:Maggie MacAlpine

Co-Founder, DEF CON Voting Village

Co-Founder, Nordic Innovation Labs

Description:No Description available

YouTube: <https://www.youtube.com/watch?v=GTiltX4vwLA>

Twitch: <https://www.twitch.tv/votingvillagedc>

Return to [Index](#) - Add to  - ics [Calendar](#) file

MOV - Friday - 09:50-09:59 PDT

Title: Welcome Speech

When: Friday, Aug 7, 09:50 - 09:59 PDT

Where: Monero Vlg

SpeakerBio:rehr

No BIO available

Description:No Description available

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Welcome to DEF CON Safe Mode

When: Friday, Aug 7, 09:30 - 09:59 PDT

Where: See Description or Village

SpeakerBio: The Dark Tangent

No BIO available

Description:

YouTube: <https://www.youtube.com/watch?v=pn68aAZc5Sg>

Twitch: <https://www.twitch.tv/defconorg>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PAYV - Friday - 09:45-09:59 PDT

Title: Welcome to the Payment Village

When: Friday, Aug 7, 09:45 - 09:59 PDT

Where: Payment Vlg

SpeakerBio: Leigh-Anne Galloway
No BIO available

Description:

Leigh-Anne will introduce you to the Payment Village and cover key information required to participate in the Payment Village at DEF CON

Payment Village activities will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/paymentvillage>

YouTube: <https://www.youtube.com/channel/UCivO-5rpPcv89Wt8okBW21Q>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What college kids always get wrong, the art of attacking newbies to blueteam

When: Thursday, Aug 6, 18:00 - 18:59 PDT

Where: Red Team VIg

SpeakerBio:Forrest Fuqua

Forrest Fuqua (JRWR) - JRWR creator of Hatchan, 3 years of NECCDC (Collegiate Cyber Defense Competition) Redteam, and defense industrial base cybersecurity pentester / auditor has been seeing all the mistakes everyone is making and works hard to try and get people to understand why its important to get your shit together.

Description:

I've done a few years at NECCDC (Collegiate Cyber Defense Competition) Red team and teams make the same mistakes over and over again with the approach of trying to harden a system that is so far compromised that it's better if they could just reinstall everything.

This talk I will detail things that have worked and not worked over the last three years that everyone seems to miss and grounds the fact that the simpler the attack. the overall better you will have in endpoints responding home. Managing rapid response to teams who are actively dealing with your malware and other tidbits.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What I Learned Trying To Hack A 737

When: Sunday, Aug 9, 16:00 - 16:59 PDT

Where: Aerospace VIg

SpeakerBio:Karl Koscher

Karl Koscher is a research scientist working at the University of Washington Security and Privacy Research Lab where he specializes in wireless and embedded systems security. He led the first team to demonstrate a complete remote compromise of a car over cellular, Bluetooth, and other channels.

Description:

As part of work looking at avionics security, we reverse-engineered two Communication Management Units used on 737s, and they are engineered unlike any other embedded system I've seen. CMUs must be certified to a high Design Assurance Level, but airlines typically want to add custom airline operations applications. This talk explores how these seemingly incompatible requirements are met in two very different ways, and takes a deep dive into how the CMUs work.

This event will be coordinated on the DEF CON Discord server, in channel #av-aviation-text.

Discord: <https://discord.com/channels/708208267699945503/732394164209057793>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What if we had TLS for phone numbers? An introduction to SHAKEN/STIR

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: Crypto & Privacy Vlg

SpeakerBio: Kelley Robinson

Kelley works on the Account Security team at Twilio. Previously she worked in a variety of API platform and data engineering roles at startups. Her research focuses on authentication user experience and design trade-offs for different risk profiles and 2FA channels. Kelley lives in Brooklyn, is an avid home cook, and spends too much time on Twitter (@kelleyrobinson).

Twitter: [@kelleyrobinson](https://twitter.com/kelleyrobinson)

Description:

If you've noticed a surge in unwanted robocalls from your own area code in the last few years, you're not alone. The way telephony systems are set up today, anyone can spoof a call or a text from any number. With an estimated 85 billion spam calls globally, it's time to address the problem. This talk will discuss the latest advancements with STIR (Secure Telephone Identity Revisited) and SHAKEN (Signature-based Handling of Asserted information using toKENS), new tech standards that use well accepted public key cryptography methods to validate caller identification. We'll discuss the path and challenges to getting this implemented industry wide, where this tech will fall short, and what we can do to limit exposure to call spam and fraud in the meantime.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Saturday - 23:00-23:59 PDT

Title: What the Shuck? Layered Hash Shucking (Rebroadcast)

When: Saturday, Aug 8, 23:00 - 23:59 PDT

Where: Password Vlg

SpeakerBio: Sam Croley (Chick3nman)

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

PWDV - Saturday - 12:00-12:59 PDT

Title: What the Shuck? Layered Hash Shucking

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: Password Vlg

SpeakerBio: Sam Croley (Chick3nman)

No BIO available

Description: No Description available

Password Village events will be streamed to both YouTube and Twitch concurrently.

Twitch: <https://twitch.tv/passwordvillage>

YouTube: https://youtube.com/channel/UCqVng_SmexXf4TW3AVdMIyQ

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: What's up with proposed privacy legislation and how to influence the debate

When: Saturday, Aug 8, 16:30 - 17:30 PDT

Where: BioHacking Vlg

SpeakerBio: Lucia Savage

Lucia Savage is nationally recognized expert on health information privacy and the difference in US health privacy law i compared to other economic sectors like ad-tech or finance. From 2014 -2017 she served as Chief Privacy Office at the HHS Office of the National Coordinator for Health IT.

Description:

In a Q/A format, with plenty of time for audience questions, Ms. Savage will explain the basic privacy legal landscape, what the hot debate topics are as people seek to change those laws nationally, and ways to influence the debate. At last count (June 4) there were three Covid-specific federal legislative proposal to oversee how commercial/ad-tech companies keep private the information they collect to help track Covid. There are approximately another 10 bills that propose to generally revamp ad-tech privacy on a national basis.

BioHacking Village activities will be streamed to Twitch and YouTube.

Twitch: <https://m.twitch.tv/biohackingvillage/profile>

YouTube: <https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: When TLS Hacks You

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: Joshua Maddux , Security Engineer, Latacora

Joshua Maddux started out as a software engineer. After a few years, having introduced his share of bugs to the world, he started hunting for vulnerabilities in his own code and elsewhere. At PKC Security he gained additional experience in software development and white-box penetration testing, and gave his first ever conference talk at Blackhat USA on a series of systemic SSRF vulnerabilities in sites supporting Apple Pay. Now on the Appsec team at Latacora, he helps advise startups in building secure products. Aside from work for clients, Joshua is also active in the bug bounty world. His past research has led to security updates in Java, Netflix, Gitlab, United Airlines, Zapier, and others.

Twitter: [@joshmdx](https://twitter.com/joshmdx)

Description:

Lots of people try to attack the security of TLS. But what if we use TLS to attack other things? It's a huge standard, and it turns out that features intended to make TLS fast have also made it useful as an attack vector.

Among other things, these features provide a lot of flexibility for Server-Side Request Forgery (SSRF). While past work using HTTPS URLs in SSRF has relied upon platform-specific bugs such as SNI injection, we can go further. In this talk, I present a novel, cross-platform way of leveraging TLS to target internal services.

Uniquely, these attacks are more effective the more comprehensively a platform supports modern TLS, so won't go away with library upgrades. It is also unlikely that the TLS spec will change overnight at the whim of a random security researcher. Instead, we need to walk through scenarios and dispel common assumptions so the audience can know what to look out for. Of course, the best way to do so is with demos!

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](https://discord.com/channels/708208267699945503/733079621402099732)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Whispers Among the Stars: Perpetrating (and Preventing) Satellite Eavesdropping Attacks

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: DEF CON Q&A Twitch

SpeakerBio: James Pavur , DPhil Student, Oxford University

James Pavur is a Rhodes Scholar at Oxford University working on a DPhil in Cyber Security. His academic research is primarily on the threats to satellite systems with a focus on satellite communications and trustworthy spaceflight operations. Prior to Oxford, he majored in Science, Technology and International Affairs (STIA) at Georgetown University where he graduated with the School of Foreign Service Dean's Medal (highest cumulative GPA) in 2017.

He has held numerous internships and professional positions related to information security. This included acting as Director of Information Security for Students of Georgetown Inc. (The Corp), a student run non-profit with more than 300 employees. He has also assisted with computer crimes investigations as an intern with the United States Postal Service Office of the Inspector General, worked on embedded systems reverse-engineering as an intern at Booz Allen Hamilton, and even pentested air-conditioners for the Public Buildings Services while working for Telos Corporation.

Outside of computers, James enjoys flying kites and collecting rare and interesting teas.

Twitter: [@JamesPavur](https://twitter.com/JamesPavur)

Description:

Space is changing. The number of satellites in orbit will increase from around 2,000 today to more than 15,000 by 2030. This briefing provides a practical look at the considerations an attacker may take when targeting satellite broadband communications networks. Using \$300 of widely available home television equipment I show that it is possible to intercept deeply sensitive data transmitted on satellite links by some of the world's largest organizations.

The talk follows a series of case studies looking at satellite communications affecting three domains: air, land, and sea. From home satellite broadband customers, to wind farms, to oil tankers and aircraft, I show how satellite eavesdroppers can threaten privacy and communications security. Beyond eavesdropping, I also discuss how, under certain conditions, this inexpensive hardware can be used to hijack active sessions over the satellite link.

The talk concludes by presenting new open source tools we have developed to help researchers seeking to improve satellite communications security and individual satellite customers looking to encrypt their traffic.

The talk assumes no background in satellite communications or cryptography but will be most interesting to researchers interested in tackling further unsolved security challenges in outer space.

This is a live Question & Answer stream. You'll want to have watched the corresponding pre-recorded talk prior to this Q&A session.

All DEF CON Q&A streams will happen on Twitch. Discussions and attendee-to-speaker participation will happen on Discord ([#track-1-live](https://discord.com/channels/708208267699945503/733079621402099732)).

Twitch: <https://www.twitch.tv/defconorg>

#track-1-live: <https://discord.com/channels/708208267699945503/733079621402099732>

Return to Index - Add to  - ics [Calendar](#) file

Title: Who needs spyware when you have COVID-19 apps? A look at global trends and what to do about it.

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: Crypto & Privacy Vlg

Speakers:C. Nadal,J. DeBlois,M. DeBlois,Z. Anderson

SpeakerBio:C. Nadal

No BIO available

SpeakerBio:J. DeBlois

No BIO available

SpeakerBio:M. DeBlois

No BIO available

SpeakerBio:Z. Anderson

No BIO available

Description:

With the current pandemic, privacy concerns have emerged around the large number of applications being published and promoted around the globe. From symptom tracking to contact tracing, the COVID-19 App Tracker Project (<https://covid19apptracker.org>) aims to automate detection of new and modified applications published on the Google Play Store.

Our session will discuss C19 app trends around the globe, emerging concerns, and what is required for greater transparency around the applications created and data collected by governments around the world.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

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

Title: Who's secure, who's not, & who makes that choice

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: AppSec Vlg

SpeakerBio:Maddie Stone

No BIO available

Twitter: [@maddiestone](https://twitter.com/maddiestone)

Description:No Description available

AppSec Village activities will be streamed to YouTube.

YouTube: <https://www.youtube.com/channel/UCpT8LI0b9ZLj1DeEQz7f0A>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Whose Slide is It Anyway

When: Saturday, Aug 8, 20:00 - 21:59 PDT

Where: See Description or Village

Description:

"Whose Slide Is It Anyway?" is 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.

But....why?

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.

Oh, and prizes. Lots and lots of prizes. Sign ups will be the day of the contest with some special ways to secure your spot early.

Forum: <https://forum.defcon.org/node/232955>

Discord: <https://discord.com/channels/708208267699945503/711644337942822925>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: wicked wardriving with gps and glonass

When: Thursday, Aug 6, 09:00 - 09:01 PDT

Where: Wireless Vlg

SpeakerBio:wytshadow

Wytshadow is a wireless security researcher who learned RF fundamentals while working for Air Force Space Command. After transitioning to the civilian world, Wytshadow became a security consultant with a specialization in wireless security where he continues to perform independent research on wireless attacks and defensive strategies on existing and emerging wireless technologies. Wytshadow has presented on independent work in the past including the wireless pentesting framework SniffAir and he also presented on attacks against WPA3 OWE.

Description:

I'll begin the talk giving my experience working in Air Force Space Command and how they fly GPS satellites. GPS is only one constellation of "GPS" satellites in space. Several other countries have their own version of GPS. Russia has GLONASS, China has Beidou, Europe has Galileo, Japan and India also have their own satellite constellations. All these satellites speak a common language known as GNSS. With the correct dongle, NOT THE BU-353, you can receive location data from more than the US controlled GPS satellites in space, this gives you more reliable location data for war driving.

I'll then go into a description of war driving with kismet and all the things kismet can collect on. I'll then show off a dongle box I slapped together that is similar to El Kentaro's kismet box. It is a pelican case with a 7 port, USB hub hot glued inside with holes drilled in it so antennas can be mounted externally.

After talking about wardriving, I'll talk about uploading results to WiGLE or uploading a kismet pcap file to google earth to keep wardrive data private. This is how you can review actively collected war drive data, but what if you want to review the work that others have done? Enter wigleQuery (<https://github.com/wytshadow/wigleQuery>). Querying WiGLE through their web interface provides a weak user experience, the access points are hard to see, even when you zoom in, and getting additional details on each access point is not very intuitive. WigleQuery provides an easier way to query WiGLE for WiFi Access Points based on BSSID(s), ESSID(s), Lat/Long and plots the result on google maps using easy to see colors and also outputs the results in CSV format for further processing. This output data can also be used when asking WiGLE admins to have your access points removed from the WiGLE database.

I'll conclude talking about future improvements to be made to wigleQuery.

This talk is available on YouTube.

Talk: <https://www.youtube.com/watch?v=2h8H3XEgWvw>

Return to Index - Add to  - ics [Calendar](#) file

Title: Wireless Blue Team

When: Thursday, Aug 6, 09:00 - 09:01 PDT

Where: Wireless VIg

SpeakerBio:Eric Escobar

Eric is a seasoned pentester and a Principal Security Consultant at Secureworks. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. He has successfully compromised companies from all sectors of business including: Healthcare, Pharmaceutical, Entertainment, Amusement Parks, Banking, Finance, Technology, Insurance, Retail, Food Distribution, Government, Education, Transportation, Energy and Industrial Manufacturing.

His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he now helps create challenges!

Description:

Wireless security is often overlooked, or deemed "good enough". However, for many companies, access to the corporate Wi-Fi means direct access to the internal network. This talk will demonstrate a variety of opening attacks performed by threat actors whose goal it is to infiltrate your organization. These tactics are detectable to the vigilant sysadmin, but all too often go unnoticed in a sea of log files. Check out this talk for access to the "Free Public WiFi".

This talk is available on YouTube.

Talk: <https://www.youtube.com/watch?v=tvYpd6sbH2g>

Return to [Index](#) - Add to  - ics [Calendar](#) file

Title: Wireless Capture the Flag

When: Friday, Aug 7, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Wireless Capture the Flag (WCTF) at DEF CON.

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 WCTF can be completely done with a little knowledge, a pen tester's determination, and \$40 or \$4000 worth of equipment; the key is to read the clues and determine the goal of each challenge.

Each WCTF event begins with a presentation: How to WCTF. There will be clues everywhere, and we will provide periodic updates. Make sure you pay attention to what's happening at the WCTF desk, on Twitter https://twitter.com/wctf_us, <https://twitter.com/rfhackers>, and the interwebz, etc. If you have a question - ASK! We may or may not answer at our discretion.

Forum: <https://forum.defcon.org/node/233017>

Discord: <https://discord.com/channels/708208267699945503/711644270976696380>

Twitter: https://twitter.com/wctf_us

Web: <https://wctf.us/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Wireless Capture the Flag

When: Saturday, Aug 8, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Wireless Capture the Flag (WCTF) at DEF CON.

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 WCTF can be completely done with a little knowledge, a pen tester's determination, and \$40 or \$4000 worth of equipment; the key is to read the clues and determine the goal of each challenge.

Each WCTF event begins with a presentation: How to WCTF. There will be clues everywhere, and we will provide periodic updates. Make sure you pay attention to what's happening at the WCTF desk, on Twitter https://twitter.com/wctf_us, <https://twitter.com/rfhackers>, and the interwebz, etc. If you have a question - ASK! We may or may not answer at our discretion.

Forum: <https://forum.defcon.org/node/233017>

Discord: <https://discord.com/channels/708208267699945503/711644270976696380>

Twitter: https://twitter.com/wctf_us

Web: <https://wctf.us/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Wireless Capture the Flag

When: Sunday, Aug 9, 09:00 - 17:59 PDT

Where: See Description or Village

Description:

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Wireless Capture the Flag (WCTF) at DEF CON.

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 WCTF can be completely done with a little knowledge, a pen tester's determination, and \$40 or \$4000 worth of equipment; the key is to read the clues and determine the goal of each challenge.

Each WCTF event begins with a presentation: How to WCTF. There will be clues everywhere, and we will provide periodic updates. Make sure you pay attention to what's happening at the WCTF desk, on Twitter https://twitter.com/wctf_us, <https://twitter.com/rfhackers>, and the interwebz, etc. If you have a question - ASK! We may or may not answer at our discretion.

Forum: <https://forum.defcon.org/node/233017>

Discord: <https://discord.com/channels/708208267699945503/711644270976696380>

Twitter: https://twitter.com/wctf_us

Web: <https://wctf.us/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

WLV - Friday - 17:45-18:45 PDT

Title: Wireless Village Fireside Talk

When: Friday, Aug 7, 17:45 - 18:45 PDT

Where: Wireless Vlg

Description:

FIRESIDE Talk, on stryngs, scapy with a dash of bluetooth, anyone want a code release and some demo on packet creation in BT and other work

#wv-general-voice: <https://discord.com/channels/708208267699945503/731262451974144071>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Wireshark for Incident Response & Threat Hunting (Beginner)

When: Saturday, Aug 8, 10:30 - 11:59 PDT

Where: Blue Team Vlg - Workshop Track 2

SpeakerBio: Michael Wylie, Director of Cybersecurity Services, Richey May Technology Solution
Michael Wylie (Twitter: @TheMikeWylie), MBA, CISSP is the Director of Cybersecurity Services at Richey May Technology Solutions. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, cloud security, penetration tests, risk management, and training. Michael has developed and taught numerous courses for the U.S. Department of Defense, DEFCON, Universities, and for clients around the world. Michael is the winner of numerous SANS challenge coins and holds the following credentials: CISSP, CCNA R&S, CCNA CyberOps, GMON, GPEN, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, Security+, Project+, and more.
Twitter: @TheMikeWylie

Description:

This workshop will take student's Wireshark skills to the next level with a heavy emphasis on incident response, threat hunting, and malicious network traffic analysis. We will begin with a brief introduction to Wireshark and other Network Security Monitoring (NSM) tools/concepts. Placement, techniques, and collection of network traffic will be discussed in detail. Throughout the workshop, we'll examine what different attacks and malware look like in Wireshark.

This workshop will take student's Wireshark skills to the next level with a heavy emphasis on incident response, threat hunting, and malicious network traffic analysis. We will begin with a brief introduction to Wireshark and other Network Security Monitoring (NSM) tools/concepts. Placement, techniques, and collection of network traffic will be discussed in detail. Throughout the workshop, we'll examine what different attacks and malware look like in Wireshark. Students will then have hands-on time in the lab to search for Indicators of Compromise (IOCs) and a potential breach to the network. There will be plenty of take home labs for additional practice.

Attendees will learn:

- How to build traffic specific Wireshark profiles - How to setup Wireshark for threat hunting - How to enrich packets with threat intel - How to identify IOCs in a sea of packets - How to tap networks and where to setup sensors - NSM techniques
- Techniques to quickly identify evil on a network

Students are provided with PCAPs of incidents starting with 8 packets and growing to 10,000+ packet captures where students need to build a timeline of a breach.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Wireshark for Incident Response & Threat Hunting

When: Saturday, Aug 8, 13:00 - 14:59 PDT

Where: Packet Hacking Vlg - Workshop

SpeakerBio: Michael Wylie, Director of Cybersecurity Services, Richey May Technology Solution
Michael Wylie (Twitter: @TheMikeWylie), MBA, CISSP is the Director of Cybersecurity Services at Richey May Technology Solutions. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, cloud security, penetration tests, risk management, and training. Michael has developed and taught numerous courses for the U.S. Department of Defense, DEFCON, Universities, and for clients around the world. Michael is the winner of numerous SANS challenge coins and holds the following credentials: CISSP, CCNA R&S, CCNA CyberOps, GMON, GPEN, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, Security+, Project+, and more.

Twitter: @TheMikeWylie

Description:

This workshop will take student's Wireshark skills to the next level with a heavy emphasis on incident response, threat hunting, and malicious network traffic analysis. We will begin with a brief introduction to Wireshark and other Network Security Monitoring (NSM) tools/concepts. Placement, techniques, and collection of network traffic will be discussed in detail. Throughout the workshop, we'll examine what different attacks and malware look like in Wireshark. Students will then have hands-on time in the lab to search for Indicators of Compromise (IOCs) and a potential breach to the network. There will be plenty of take home labs for additional practice.

This workshop requires registration. If you are registered, please proceed to #phv-infobooth-text and you'll be given access to join.

#phv-infobooth-text: <https://discord.com/channels/708208267699945503/708242376883306526>

Return to Index - Add to  - ics [Calendar](#) file

Title: Workshop: Let's Talk About Abusability Testing

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: Crypto & Privacy Vlg

Speakers: Avi Zajac, Franchesca Spektor, Ji Su Yoo, Nicole Chi

SpeakerBio: Avi Zajac

Avi (@_llzes, Avi/they/he) is a privacy-focused hacker and engineer. They love rabbits, cheesecake, and cute things like privacy and security, locksport, cryptography.

Twitter: [@_llzes](#)

SpeakerBio: Franchesca Spektor

Franky's (@3llsaria, she/her) expertise is in ethical design practices around bioethics, disability & sexuality, and she previously served as a Lab Manager for the Disability Design Lab at UC Berkeley.

SpeakerBio: Ji Su Yoo

Ji Su (she/her) is a PhD at UC Berkeley's School of Information and former researcher at the Harvard Data Privacy Lab, where she worked on security protocol and data privacy.

SpeakerBio: Nicole Chi

Nicole's (@tinween, she/her) focus is on the "tech for good" space in its many forms, having worked in civic tech, nonprofit digital capacity building, tech policy, and ML ethics. Her strength is bridging connections and expertise across disciplines.

Twitter: [@tinween](#)

Description:

Are you concerned about how your products may be used for harm: intentionally or unintentionally? We will be covering the concept of abusability testing for platform abuse in this hybrid panel and workshop, with a clicker style method of interacting to foster deep understanding and participate in discussions on abusability testing. You'll walk away with an understanding of abusability testing, join a community passionate about fighting platform abuse, and maybe walk away with actionable steps you can take to alleviate harm in your own products.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Workshop: Let's Talk About Abusability Testing

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: Crypto & Privacy VIg

Speakers: Avi Zajac, Franchesca Spektor, Ji Su Yoo, Nicole Chi

SpeakerBio: Avi Zajac

Avi (@_llzes, Avi/they/he) is a privacy-focused hacker and engineer. They love rabbits, cheesecake, and cute things like privacy and security, locksport, cryptography.

Twitter: [@_llzes](#)

SpeakerBio: Franchesca Spektor

Franky's (@3llsaria, she/her) expertise is in ethical design practices around bioethics, disability & sexuality, and she previously served as a Lab Manager for the Disability Design Lab at UC Berkeley.

SpeakerBio: Ji Su Yoo

Ji Su (she/her) is a PhD at UC Berkeley's School of Information and former researcher at the Harvard Data Privacy Lab, where she worked on security protocol and data privacy.

SpeakerBio: Nicole Chi

Nicole's (@tinween, she/her) focus is on the "tech for good" space in its many forms, having worked in civic tech, nonprofit digital capacity building, tech policy, and ML ethics. Her strength is bridging connections and expertise across disciplines.

Twitter: [@tinween](#)

Description:

Are you concerned about how your products may be used for harm: intentionally or unintentionally? We will be covering the concept of abusability testing for platform abuse in this hybrid panel and workshop, with a clicker style method of interacting to foster deep understanding and participate in discussions on abusability testing. You'll walk away with an understanding of abusability testing, join a community passionate about fighting platform abuse, and maybe walk away with actionable steps you can take to alleviate harm in your own products.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

Return to Index - Add to  - ics [Calendar](#) file

Title: Workshop: Let's Talk About Abusability Testing

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: Crypto & Privacy VIg

Speakers: Avi Zajac, Franchesca Spektor, Ji Su Yoo, Nicole Chi

SpeakerBio: Avi Zajac

Avi (@_llzes, Avi/they/he) is a privacy-focused hacker and engineer. They love rabbits, cheesecake, and cute things like privacy and security, locksport, cryptography.

Twitter: [@_llzes](#)

SpeakerBio: Franchesca Spektor

Franky's (@3llsaria, she/her) expertise is in ethical design practices around bioethics, disability & sexuality, and she previously served as a Lab Manager for the Disability Design Lab at UC Berkeley.

SpeakerBio: Ji Su Yoo

Ji Su (she/her) is a PhD at UC Berkeley's School of Information and former researcher at the Harvard Data Privacy Lab, where she worked on security protocol and data privacy.

SpeakerBio: Nicole Chi

Nicole's (@tinween, she/her) focus is on the "tech for good" space in its many forms, having worked in civic tech, nonprofit digital capacity building, tech policy, and ML ethics. Her strength is bridging connections and expertise across disciplines.

Twitter: [@tinween](#)

Description:

Are you concerned about how your products may be used for harm: intentionally or unintentionally? We will be covering the concept of abusability testing for platform abuse in this hybrid panel and workshop, with a clicker style method of interacting to foster deep understanding and participate in discussions on abusability testing. You'll walk away with an understanding of abusability testing, join a community passionate about fighting platform abuse, and maybe walk away with actionable steps you can take to alleviate harm in your own products.

Crypto & Privacy Village activities will be streamed to YouTube and Twitch.

Twitch: <https://twitch.tv/cryptovillage>

YouTube: <https://www.youtube.com/channel/UCGWMS6k9rg9uOf3FmYdjwwQ>

Return to Index - Add to  - ics [Calendar](#) file

Title: Writing Wireshark Plugins for Security Analysis

When: Saturday, Aug 8, 09:00 - 10:59 PDT

Where: Packet Hacking Vlg - Workshop

Speakers: Jeswin Mathai, Nishant Sharma

SpeakerBio: Jeswin Mathai , Security Researcher, Pentester Academy

Jeswin Mathai (Twitter: @jeswinmathai) is a Researcher at Pentester Academy and Attack Defense. He has presented/published his work at DEF CON China, Blackhat Arsenal and Demo labs (DEFCON). He has a Bachelor's degree from IIIT Bhubaneswar. He was the team lead at InfoSec Society IIIT Bhubaneswar in association with CDAC and ISEA, which performed security auditing of government portals, conducted awareness workshops for government institutions. He was also the part of team Pied Piper who won Smart India Hackathon 2017, a national level competition organized by GoI. His area of interest includes Malware Analysis and Reverse Engineering, Cryptography, WiFi security and Web Application Security.

Twitter: @jeswinmathai

SpeakerBio: Nishant Sharma , R&D Manager, Pentester Academy

Nishant Sharma (Twitter: @wifisecguy) is an R&D Manager at Pentester Academy and Attack Defense. He is also the Architect at Hacker Arsenal where he leads the development of multiple gadgets for WiFi pentesting such as WiMonitor, WiNX and WiMini. He also handles technical content creation and moderation for Pentester Academy TV. He has 7+ years of experience in information security field including 5+ years in WiFi security research and development. He has presented/published his work at Blackhat USA/Asia, DEF CON China, Wireless Village, IoT village and Demo labs (DEFCON USA). Prior to joining Pentester Academy, he worked as a firmware developer at Mojo Networks where he contributed in developing new features for the enterprise-grade WiFi APs and maintaining the state of art WiFi Intrusion Prevention System (WIPS). He has a Master's degree in Information Security from IIIT Delhi. He has also published peer-reviewed academic research on HMAC security. His areas of interest include WiFi and IoT security, AD security, Forensics and Cryptography.

Twitter: @wifisecguy

Description:

Network traffic always proves to be a gold mine when mined with proper tools. There are various open source and paid tools to analyze the traffic but most of them either have predefined functionality or scalability issues or one of a dozen other problems. And, in some cases when we are dealing with non-standard protocols, the analysis becomes more difficult. But, what if we can extend our favorite traffic analysis tool Wireshark to accommodate our requirements? As most people know, Wireshark supports custom plugins created in C and Lua which can be used to analyze or dissect the packets. In this workshop, we will learn the basics of Wireshark plugins and move on to create different types of plugins to perform dissection of non-standard protocol, provide macro statistics, detect attacks etc. We will use examples of older and newer protocols (including non-standard ones) to understand the plugin workflow and development.

This workshop requires registration. If you are registered, please proceed to #phv-infobooth-text and you'll be given access to join.

#phv-infobooth-text: <https://discord.com/channels/708208267699945503/708242376883306526>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Y'all Tryna Bypass Python 3.8 Audit Hooks or Nah?

When: Saturday, Aug 8, 09:45 - 10:45 PDT

Where: Red Team VIg

SpeakerBio:Leron Gray

Leron Gray is a ten year Navy veteran and former NSA operator with six years of offensive security experience. He's currently works on the Azure Red Team at Microsoft, loves winning all the CTFs, and enjoys writing things in Python and Pythonic languages. Also a dope rapper. #BARS

Description:

Python 3.8, released October 2019, boasts a new security feature called “audit hooks . According to PEP 578 and PEP 551, the purpose of audit hooking is to allow transparency into Python’s runtime so that events can be monitored and logged just like any other process. While additional insight is great for defenders, it's likely to become another hurdle for attackers to overcome in the same vein as PowerShell. Y'all tryna bypass these audit hooks or nah? Come through.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

HTS - Friday - 10:00-10:30 PDT

Title: Yacht PWNed

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: Hack the Sea VIg

SpeakerBio: Stephen Gerling

No BIO available

Description: No Description available

Hack the Sea Village activities will be streamed to Twitch.

Twitch: <https://twitch.tv/hackthesea>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Yippee-Ki-Yay MFA'er - Bypassing Multi-Factor Authentication with Real-Time Replay Session Instantiation Attacks

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: Red Team Vlg

Speaker Bio: Justin Hutchens (“Hutch”)

Justin Hutchens (“Hutch”) is a seasoned cyber-security professional who specializes in vulnerability management, attack simulations, penetration testing, and red teaming. In 2008, Hutch began his information security career doing Threat and Vulnerability Management for the United States Air Force. Since separating from the Air Force, he has gone on to lead multiple penetration testing teams in both consulting and internal capacities. He has also achieved a Master’s degree in Computer Security Management and multiple information security certifications to include CISSP, GPEN, GWAPT, and OSCP. Hutch has significant experience in the field and has led assessments in nearly every industry and vertical. He is skilled in coding in Python, JavaScript, PowerShell, and Bash -- and emphasizes the importance of automation for both assessment methodology and development of internal processes.

Description:

In the not-too-distance past, it was fairly easy for red-teamers to conquer almost any environment with a combination of password sprays, or by leveraging social engineering to lure victims to fake login sites and harvest their credentials. But in the current landscape, there are new road-blocks to contend with. Nearly every company and organization has now deployed some form of Multi-Factor Authentication (MFA) on their perimeter services. Fortunately, for red-teamers, the vast majority of implementations of MFA across the Internet (email-based, SMS, OTP, and push requests) all share a common critical flaw that can still be easily circumvented using a modern revision of the classic “credential harvesting attacks. This talk will offer a comprehensive methodology for how a red team can effectively bypass nearly any MFA service using Python-Flask and browser emulation libraries (Mechanize or Selenium) to replay MFA credentials in real-time, establish legitimate user sessions, and then harvest the session tokens to assume access to those compromised sessions. This methodology will prove once again, that the advantage is still square in the hands of the red team, and that even now...ALL YOUR BASE ARE BELONG TO US!!!

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: You're Adversary Within - The Golden Age of Insider Threats

When: Sunday, Aug 9, 13:30 - 14:30 PDT

Where: Red Team Vlg

SpeakerBio: Adam Mashinchi

Adam Mashinchi is SCYTHE's VP of Product Management where he leads the project management, design, and quality assurance departments for SCYTHE's product portfolio. Before SCYTHE, Adam defined and managed the development of enterprise security and privacy solutions with an emphasis on usable encryption at a global scale and led numerous technical integration projects with a variety of partners and services.

Twitter: [@adam_mashinchi](https://twitter.com/adam_mashinchi)

Description:

Intentional read as both “Your Adversary Within” and “You Are (The) Adversary Within” attendees of this talk will walk away with practical information on how to execute advanced insider threat scenarios with free and easily implemented solutions.

With the increased enterprise dependence on cloud-based solutions, paired with turn-key end-to-end encryption products for consumers; insider threat actors have a litany of tools at their disposal. In this talk we will walk-through a number of the (free!) tools one can utilize when performing adversarial simulations, provide insights on how to “sell” an assumed-compromise engagement as a Red/Blue/Purple Team, and some helpful places to start with MITRE ATT&CK technique alignment for offense & defense.

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteammillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

MOV - Sunday - 12:00-12:30 PDT

Title: You're not the money printer, or why we need to separate coinbase rings

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: Monero Vlg

SpeakerBio:sgp

No BIO available

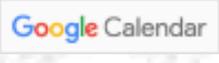
Description:No Description available

Monero Village activities will be streamed to Twitch and YouTube.

Twitch: <https://www.twitch.tv/monerovillage/>

YouTube: <https://www.youtube.com/c/monerocommunityworkgroup/>

#mv-general-text: <https://discord.com/channels/708208267699945503/732733510288408676>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Your connected world isn't yours anymore! - Remote IoT attacks and data exfiltration.

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: IOT Vlg

Speakers:Dewank Pant,Shruti Lohani

SpeakerBio:Dewank Pant

Dewank Pant is a Security Engineer working with NCC Group Inc. He graduated from and worked at Johns Hopkins University under the Information Security Track. He is skilled in IoT Security, Radio Hacking, Bot Development, and penetration testing. He has published several CVEs and holds 3+ years of work experience in the industry.

SpeakerBio:Shruti Lohani

Shruti Lohani is a Computer Scientist working in IoT Research & Development in the sectors of Energy, Petrochemical, Aerospace, Automotive, etc. at Nexess, France. She completed her M.Sc. from EURECOM, France and has 3 years of experience in the IoT domain. Her expertise in IoT application and security is not limited to Smart homes, autonomous vehicles, indoor/outdoor Geolocation.

Description:

From smart home devices to smart cars, IoT actually gave us our “connected world”, but maybe not a “Safe” one. Imagine all your smart devices on your home network being controlled by someone on the other side of the world, your smart TVs, smart lights, baby monitors, routers, printers, workspace surveillance cameras, and literally everything else!

This talk explores how the methods of manipulating domain name resolution can be used to exploit and remotely take over most of the connected devices in a private network. We will talk about how it can be used to scan a private network externally for IoT devices, and how it can put even private devices open to the public! We will cover some tools that can be used to takeover a device and exfiltrate the data of a victim under a minute with minimum user interaction. We demonstrate how the data can be exfiltrated and used to perform unwanted actions on the victim's devices from anywhere in the world.

We furthermore, talk about methods of prevention and best practices that a developer and product designer can consider to protect their devices against such attacks. So if you're a pentester or a developer we've got something for everyone!

IOT Village activities will be streamed to Twitch.

Twitch: <https://www.twitch.tv/iotvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Zebbler Encanti Experience

When: Friday, Aug 7, 21:00 - 21:59 PDT

Where: See Description or Village

Description:

Zebbler Encanti Experience (aka ZEE) is an audio/visual collaboration between video artist Zebbler and electronic music producer Encanti, based out of Boston and the Scottish Highlands. The Experience is a performance of mapped visuals on three custom winged projection screens, synchronized with heavy peak-hour psychedelic bass music, resulting in the creation of an immersive A/V fantasy world.

Forum: <https://forum.defcon.org/node/230970>

Discord: <https://discord.com/channels/708208267699945503/735624334302904350>

Location: https://www.twitch.tv/defcon_music

Web: <http://zebblerencantiexperience.com/>

Facebook: <https://www.facebook.com/zebblerencantiexperience>

Instagram: <https://www.instagram.com/zebblerencantiexperience/>

[Return to Index](#) - Add to  - ics [Calendar](#) file

Title: Zeek: An Introduction Into OpenSOC CTF Tools

When: Thursday, Aug 6, 15:15 - 15:59 PDT

Where: Blue Team VIg - Workshop Track 1

Speakers: Aaron Soto, Amber Graner

SpeakerBio: Aaron Soto

Aaron Soto is at Corelight, training users on the Zeek (formerly Bro) network monitoring platform. He was recently on Rapid7's Metasploit team. In his off-time, he enjoys endurance automotive racing, ham radio, and helping at the DEF CON OpenSOC Blue Team Village CTF.

Twitter: [@_surefire_](#)

SpeakerBio: Amber Graner

No BIO available

Description:

Learn. Play. Do.

Every year the Blue Team Village hosts OpenSOC. A unique defense CTF meant to teach and test practical incident response skills in an environment that's as close to "the real thing" as it gets.

This year BTV wanted to do more. We know that some Blue Teamers might be unfamiliar with some of the tools used by OpenSOC. And we didn't want that to keep anyone from playing this incredible defense simulation.

So this year we are dedicating all day Thursday to demo the various OpenSOC tools, before OpenSOC starts on Friday. These are tools like Graylog, Moloch, Zeek, Osquery, and others that Blue Teamers rely on every day to defend their networks against attackers.

That means that after you LEARN the tools, you can PLAY the OpenSOC CTF, and then take that knowledge back to your own Blue Team to DO the work of defending your network.

This is a workshop that requires pre-registration. Details for how to participate in this workshop can be obtained by contacting the Blue Team Village staff.

[Return to Index](#) - Add to  - ics [Calendar](#) file

RTV - Thursday - 16:45-17:45 PDT

Title: Zero Trust - A Vision for Securing Cloud and Redefining Security

When: Thursday, Aug 6, 16:45 - 17:45 PDT

Where: Red Team VIg

SpeakerBio: Vandana Verma Sehgal

No BIO available

Twitter: [@InfosecVandana](#)

Description: No Description available

Red Team Village events will be streamed to YouTube and Twitch.

Twitch: <https://www.twitch.tv/redteamvillage>

[Return to Index](#) - Add to  - ics [Calendar](#) file

DEF CON Discord: <https://discord.gg/defcon>

DEF CON 28 SAFE MODE Artwork Contest Winners!

Posted 8.7.20



We want to offer our heartfelt thanks to everyone who entered the DEF CON Safe Mode Art Contest. We're always amazed at the level of talent in this community.

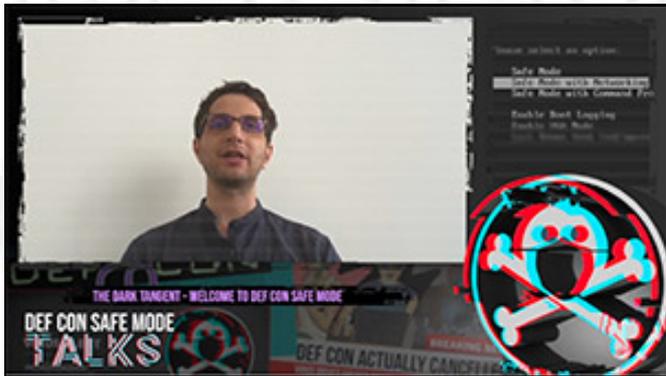
This year's runner up is a stylish meditation on the profusion of connectivities that characterize modern life by Rita Tu.

Much like Highlanders, however, in the end there can be only one. This year's highlander is @hannahdiazart. The entry has both wide-eyed discovery (very on theme) and boxes full of random electronics (super relatable). Also a robot dinosaur. It communicates something about the hacker spirit that is both warm and life-affirming.

Congratulations to Hannah and Rita and thanks again to everyone who participated.

SAFE MODE Content is Live!

Posted 8.5.20



To get the party started, we're releasing a bunch of the content early. Over on the [media server](#), we've got all of the main stage talks and materials, the soundtrack, demo labs, art, CTF, music - take what you like. Completists out there, we see you. There's a very thicc torrent file as well. Take some time to watch the talks you've been waiting for at your leisure, so you're ready for the live Q&A sessions starting Thursday. This will be the first DEF CON where you won't have to pick between main stage talks and the rest of the show, so take advantage. If you had plans, we apologize.

So close now!

Upgrade to Human Plus, and Show your Support!

Posted 8.4.20



DEF CON Safe Mode is almost here! We hope you're as excited as we are. For everyone looking to support DEF CON in this unusually difficult time, we have a new option for you to consider - Human PLUS.

Safe Mode is free to all Humans, but you can upgrade to Human Plus for \$20 USD on the DEF CON Discord for a few upgraded privileges. You get stuff like the ability to post pics and links, change your nick, access to Plus only chill out rooms and the good feeling that you've helped keep DEF CON alive until we meet again in Vegas. The information is all spelled out on <https://defcon.org/dc-safemode-plus.html> .

Your support makes DEF CON possible, and we appreciate all the encouragement and enthusiasm you've brought to this first-time online event. Thanks for sticking with us - we can't wait until we get to do it again in person. DEF CON hearts you.

DEF CON Safe Mode Villages Are Live!

Posted 7.28.20



More DEF CON Safe Mode News - The [Villages Page is LIVE](#) ! Check out the 30 (!) villages that are taking part and start planning your Con. Links are provided to the appropriate DEF CON forum nodes for each village and the various info you'll need to participate. We're almost there, people. #getpsyched!

Demo Labs are Back for Safe Mode!

Posted 7.24.20



The ever-popular DEF CON Demo Labs are returning for #defconsafemode! Support open-source hotness and the work of your fellow hackers and maybe even get some inspiration for your own projects. The full list of offerings is live on the [DEF CON Demo Labs Page](#) !

Check out the DEF CON Safe Mode Speaker Page and Schedule!

Posted 7.23.20



It's #defconsafemode alert time again! The [main track talk schedule](#) and [speaker page](#) for #defcon28 is now #live! Permission to get psyched is #granted. More announcements on the way!

This. Is. Happening.

DEF CON Safe Mode Music Lineup!

Posted 7.21.20



Here at the DEF CON Research Institute, we've been working hard to unlock the perfect blend of mind-expanding content and sweaty dancefloor abandon that makes the perfect Con experience. You'll be happy to know that we're applying that research to the #defconsafemode experiment.

Friday and Saturday night, we'll be providing tasty beats from the likes of Miss Jackalope, Skittish and Bus and Ninjula. Head over to the [Safe Mode Entertainment Page](#) for the complete lineup.

DEF CON Safe Mode Badges are Here!

Posted 7.16.20



The DEF CON Safe Mode badge is here! This year's model is created by the inimitable LostboY, veteran DEF CON badge and Mystery Challenge creator. While the physical format may be unfamiliar to the youngest among you, seasoned players will recognize it as a 'cassette tape' - an analog recording format consisting of a ribbon of magnetic tape and a plastic housing to keep your dirty fingers away from said tape. [More on the DEF CON Safe Mode Badge Page](#)

DEF CON Safe Mode Link Roundup!

Posted 7.14.20



DEF CON Safe Mode is almost here! If you're just getting around to checking out the offerings, here's a little roundup of the stuff you need to know.

Visit the Forums: The planning for the many events of DEF CON Safe Mode is all happening on the DEF CON Forums. Whether you want to register for an event, offer to help out with a village, or just get a start on planning your DC weekend, you can find the relevant thread in the [DC28 planning forum](#).

#Badgeliflife is still in effect: The DEF CON community creates a lot of really amazing badges, many of which are available for sale and/or trade. You can catch up with the community badges on the [DEF CON Forums #badgeleife thread](#). You can also follow the hashtag #badgeliflife on Twitter and Instagram.

Of course, DEF CON has a badge this year, too. We'll be announcing it quite soon. It's the creation of returning puzzle master LosT (@1o57), so you'll want to set aside some time to unock its mysteries.

Swag: If you're wondering how to get your hands on DEF CON Safe Mode swag this year, we've got you covered over on the [DEF CON eBay store](#)!

So dive in! Get yourself set up on Discord and Twitch, fire up the DEF CON stream on [soma fm](#) for some musical inspiration and get your mind right. DEF CON 28 will be upon us before you know it.

NEW Safe Mode Swag in the Shop!

Posted 7.2.20



We've got some brand new #DEFCONSafeMode items available at the [DEF CON eBay store](#) - a very cool pin, new flag, and a new tee and hoody with our beloved Jack in #glitchmode. Tighten up your Zoom game with a fresh new look!

Badgeline on the DEF CON Forums!

Posted 6.28.20



Attention #Badgeline enthusiasts - the #DEFCONForums has a [dedicated thread](#) for people who want to talk badges , including #safemode badges. Share, swap, sell, window-shop - join the conversation!

DEF CON Short Story Contest Still Open! Only One Week Left!

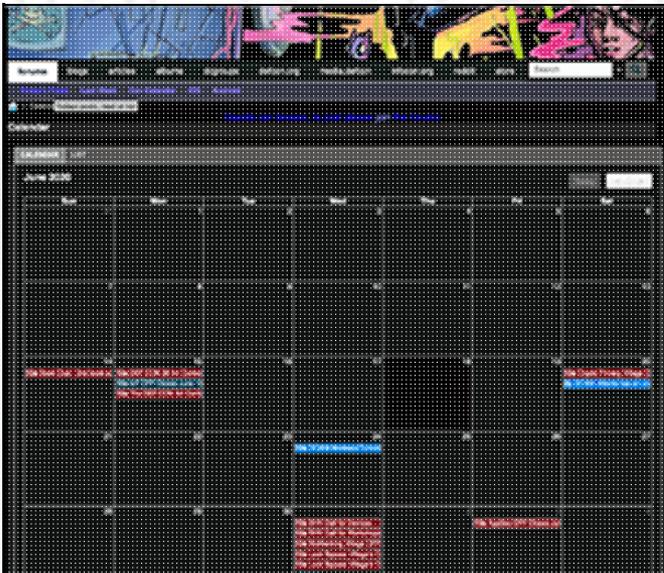
Posted 6.23.20



Reminder to all the hacker scribes out there - the [DEF CON Safe Mode Short Story Contest](#) closes July 1! Don't let procrastination rob you of your chance at glory and fabulous prizes!

Check Out the Con Calendar!

Posted 6.17.20



DEF CON Safe Mode Reminder:

We're keeping [a calendar over on the DEF CON Forums](#) with all the deadlines for content. As a bunch of these deadlines are imminent, it's worth throwing a bookmark down on it. While you're there you can also get involved in all sorts of planning discussions - your help and feedback are a big part of making this happen. Don't miss the opportunity to help shape DEF CON Safe Mode.

New DEF CON is Canceled Swag Up on our eBay Store!

Posted 6.9.20



Swag alert! The [DEF CON store](#) has a ton of new #DEFCONisCanceled goodies for your delectation. The much requested mask is here, along with hats, pins and stickers. Thanks to everyone for your support while we construct #defconsafemode - stay tuned for even more new swag items in the coming days! Stay safe, and stay in touch.

DEF CON SAFE MODE Village Activity is Growing!

Posted 5.29.20



DEF CON Safe Mode is growing fast - check out these links to some of the Villages that are signing up to take part! New CFPs are opening up by the day. But don't stop there - jump into [the forums](#) and join the discussion. Your feedback is a crucial part of creating a great Con, so join us as we build this thing out. Exciting, ain't it?

From IOT Village: >> <https://twitch.tv/iotvillage> << Make sure to follow IoT Village on Twitch to get updates about our talks that go live on May 28th and 29th along with the talks that will be hosted there later this year for our @defcon CFP!!!
<https://twitter.com/iotvillage/status/1262574224855744514?s=21>

From Crypto and Privacy Village (@CryptoVillage) : We're back! Our Call for Participation is officially open! For details on the Crypto & Privacy Village: Glitched CFP - check out our site!
<https://twitter.com/CryptoVillage/status/1263184313861865473>

From ICS Village: Submit your CFP @defcon for the Village!
https://twitter.com/ICS_Village/status/1265653986230763520

From the Voting Village: Reminder: @defcon Voting Machine Hacking Village @VotingVillageDC speaker track CFP is OPEN! Call for Papers deadline June 12, 2020, at 5:00 PM PT
More information : <https://forum.defcon.org/node/232527#post232527>

DEF CON eBay Store is Back!

Posted 5.28.20



The [DEF CON eBay store](#) is back online! Thanks for bearing with us while we got everything sorted out. DEF CON Safe Mode merchandise (and all other DC merch, for that matter) will be available only on the DEF CON eBay store.

Stay tuned for new #defconiscanceled items, stay safe, and stay in touch with us on the DEF CON FORUMS!

2020 DEF CON CTF Quals Results!

Posted 5.18.20



Congratulations to A*O*E, the winners of the DEF CON Safe Mode CTF Qualifiers, and our heartfelt thanks to the amazing team at Order of the Overflow for hosting a great event.

This year's @defcon Quals are over, but you don't have to stop yet! The scoreboard has been made static and the challenges are still available! Everyone can see challenge info, interact with the challenges (they'll stay up for a few days) and check the flags they can retrieve!//

<https://scoreboard.ooverflow.io/#/@ooverflow>

2020 DEF CON CTF Quals are about to go live!

Posted 5.15.20



The moment has arrived - the DEF CON CTF Quals are happening TODAY! Winner gets a seat at the DEF CON Safe Mode CTF event and a shot at everlasting glory. We wish the best of luck to all the contestants. Stay up to date with all the CTF updates by following our brilliant hosts, Order of the Overflow.

Godspeed, one and all.

<https://www.ooverflow.io/>
[@ooverflow](#)

DEF CON Safe Mode Swag Update - Women's Shirts Added

Posted 5.11.20

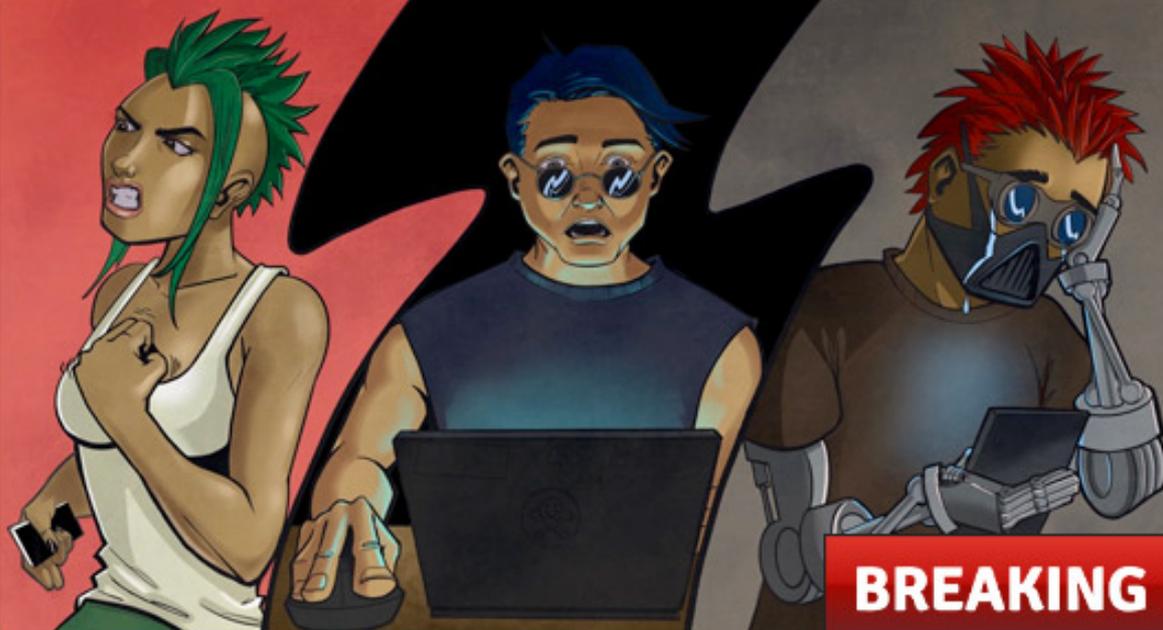


We've updated the [DEF CON Safe Mode Swag page](#) with Women's cut shirts.

We're gratified by the response from the hacker community and we're working to create more options for commemorating #defconsafemode. Keep checking our site for updates. Thanks for your patience.

DEF CON 28 has entered Safe Mode.

LIVE



BREAKING NEWS

DEF CON ACTUALLY CANCELED?

WTF

VIRUS DRIVES HACKER CONFERENCE TO THE 'INTERNET'

The 'DEF CON is canceled' meme has crossed over into real life, courtesy of COVID-19. In early March we had hopes that things would be stable by August. That is no longer realistic. Currently there's no way to gather everyone together and keep them safe, so The Dark Tangent has decided to cancel the in-person event.

We will try an experiment this year - an online DEF CON. Please read [The Dark Tangent's more detailed thoughts](#) on the situation and then head over to [the Forums to get involved](#). There is a [DEF CON Safe Mode FAQ](#) that should help to answer common questions.

We wish there was better news, but we hackers are a resilient bunch. Stay healthy, stay safe, and stay in touch so we can all be together virtually this August 6-9 and again for DEF CON 29 in person.

[Return to Index](#)

© 1992-2020 DEF CON Communications, Inc. All Rights Reserved | [DEF CON Policies](#)

DEF CON 28 FAQ

DEF CON 28 Safe Mode FAQ

Is DEF CON 28 really canceled?

Yes, for really real this time. For the health and safety of our community, the decision has been made to put DEF CON 28 into “safe-mode with networking”. The DEF CON in-person conference scheduled August 6-9, 2020 has been canceled.

See the announcement here: <https://forum.defcon.org/node/232005>

Black Hat USA also has an update to their plans. Details here: <https://www.blackhat.com/us-20/updates.html>

How do I find out about virtual events?

Even though our in-person Las Vegas event is canceled, we will run DEF CON 28 Safe Mode August 7-9 (Friday through Sunday) with 101 orientation Thursday - all of it remote. We will use the DEF CON Forums to coordinate all the various ways for you to participate. That is where everyone can announce their plans, do signups, post pictures and videos and get people involved.

Then on August 6th we will open the [DEF CON discord.gg/defcon server](https://discord.gg/defcon) up for everyone to join and start their con experience!

Will there be any SWAG?

[Always.](#)

What happens with my hotel reservation?

If you made a reservation within the official DEF CON hotel block (Caesars Palace, Harrahs, Linq, Flamingo, Planet Hollywood, Paris, Bally's, Cromwell), your reservation will automatically be canceled by Caesars Entertainment and you will be notified by email. If you made a reservation outside of our DEF CON group block, please contact the hotel directly to cancel your reservation.

What about DEF CON 29?

DEF CON 29 is scheduled for August 5-8, 2021. You can reserve [DEF CON 29 hotel rooms](#) now.

What about my DEF CON 28 content submission?

DEF CON 28 on-site is officially canceled, however DEF CON talks, workshops, demo labs, and training CFPs submissions will be processed on schedule as originally planned.

Will I get feedback on my content submission(s)?

Yes, please review the details in your status email for feedback information. CFP, training, workshops and demo labs status emails should all arrive as originally planned in the first weeks of June, if not earlier. We will post an update via official DEF CON accounts when all applications have been notified.

Will my DEF CON 28 application be considered valid for DEF CON 29?

No, you will have to submit a fresh form when the DEF CON 29 calls for content open. Too much time will have passed and we want to make sure you have made updates to keep it fresh.

Will there be a virtual talk track? What about demo labs, workshops or training?

We don't know yet, but are reviewing options internally. If your application meets our standard criteria for acceptance we will communicate options with you directly.

What about Honorariums for virtual content?

Payment Honorariums, badge(s) or check(s), will still be honored for talks, workshops, demo labs, and training. Honorariums in form of entry Badge(s) will carry over for DEF CON 29 in 2021, but travel and accommodations will not.

I'm a contest, event, village, etc., how can I share content?

We plan to organize everything [here on the DEF CON Forums](#), and then on August 6th we will open the [DEF CON discord.gg/defcon server](#) up for everyone to join and start their con experience! DEF CON Safe Mode will then run August 7-9 (Friday through Sunday) with 101 orientation Thursday.

Content organizers that want to run a virtual event, contest, or party are encouraged to use the DEF CON Forums as a hub to connect with attendees and share plans. Since last year we have added photo albums, video upload support, along with a mobile app. If you wish to have a forums presence please read the rules, create an account, and get started. We recommend reading the [forums planning announcement](#) too.

For the DEF CON DISCORD: Everyone who organizes content could have their own discord category to control and manage. Content creators can moderate what they want in their category; streaming, files, 10 different chat channels, whatever. We will help you do this.

What if I'm a party, meetup, or event organizer?

If you come up with an alternative virtual event, zoom meeting, AR chat, etc please notify us and coordinate via the DEF CON Forums. We will have an open call for hosted parties and social activities to build a calendar of events with links. We would love to hear from you.

I'm a vendor, what's next?

Please check your email for a direct mail from our Vendors department. To participate in the 2021 event, you will need to submit a DC29 vendor application. Call for DC29 vendors will open February 1st, 2021. Please contact [vendors\(at\)defcon\(d0t\)org](mailto:vendors@defcon(d0t)org) directly if you've questions.

I'm an Entertainer or Musician, what about my application?

Are you interested in a remote performance or contributing music for our DEF CON Is Canceled album? We would love to hear from you. Those who've already applied, we will be in touch. If you have any questions please email us at [info\(at\)defcon\(d0t\)org](mailto:info@defcon(d0t)org).

Is there a DEF CON Is Canceled theme song?

Yes, from the DEF CON 25 Audio CD, [01 - Skittish and Bus - DEF CON Is Canceled.m4a](#)

You can download the whole album from media.defcon.org.

[DEF CON 25 Music CD - aac 224k/](#)

[DEF CON 25 Music CD - flac/](#)

[DEF CON 25 Music CD - opus 384k/](#)

I have a question that's not answered.

If you have a question not answered here you can email [Info\(at\)defcon\(d0t\)org](mailto:Info@defcon(d0t)org), we will connect you with the right team. You may also reach out directly to the DEF CON contact that relates to your need, you can find contact info for most everyone and anything on "[Calls for Everything](#)".

[Return to Index](#)

© 1992-2020 DEF CON Communications, Inc. All Rights Reserved | [DEF CON Policies](#)

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 28 will be held August 6th through August 9th at a the brand new Caesars Forum in Las Vegas, as well as Flamingo, Linq, and Harrah's. 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 can be found at <http://defcon.stotan.org/faq/>

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?

Sadly, DEF CON 28 in-person is cancelled due to COVID-19. Check out [DEF CON Safe mode w/ networking](#) for our virtual offerings.

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 (call for papers). 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@defcon.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 28 is TBA. For reference, DEF CON 27 cost \$300 USD Cash for all four days. Do we take credit cards? Are you JOKING? No, we only accept cash - no checks, no money orders, no travelers checks. We don't want to be a target of any State or Federal fishing expeditions.

Does my underage child need a badge?

Children under the age of 8 will not need to purchase a badge.

Can I pre-register for DEF CON?

No. We used to do this a long time ago, but found that managing the registration list, and preventing one 'Dr. Evil' from impersonating another 'Dr. Evil' too much of a hassle. Seeing how we would only take cash in the first place, and things becomes time consuming and easy to abuse. Cash at the door works every time.

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?

DEF CON is cheaper than many concerts, and certainly cheaper than many shows in Vegas. 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 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 28 group room registration is now live! We have room rates at seven hotels, until they run out of rooms in our block.

Follow this link: <https://book.passkey.com/go/SHDEF0>

Do not worry if the form doesn't immediately show the discounted rate. To verify that you're getting our price you can mouse over the dates you've selected or begin the checkout process.

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 successfully streamed all tracks to all the hotels, and a couple of tracks out to the internet, for several years now. We don't expect this will change!

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. The hotel is 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](#)

© 1992-2020 DEF CON Communications, Inc. All Rights Reserved | [DEF CON Policies](#)

Links to DEF CON 28 related pages

Links

DEF CON . org

[Main DEFCON site](#)

[DEFCON 28](#)

[DEFCON 28 FAQ](#)

[DEFCON FAQ](#)

[DEFCON 28 Schedule and Speakers pages](#)

[DEFCON 28 Contest & Events](#)

[DEFCON 28 Demolabs Schedule](#)

[DEFCON 28 Entertainment](#)

[DEFCON 28 Villages](#)

village info derived from the following pages

[DEF CON 28 Villages page](#)

[DEF CON 28 Villages Forum page](#)

Thanks to the InfoBooth crew for providing access to their backend database. <claps> to their hard work!

Villages

Village Name	Forum Link	DC Village Desc	Discord Chan	Soc Media Links
AI Village	Forum	AIV Desc	#aiv-general-text	TW @AIVillage_DC
AeroSpace Village Hack-A-Sat	Forum	AEV Desc	#av-lounge-bar-text	TW @SecureAerospace TW @Hack-A-Sat
AppSec Village	Forum	ASV Desc	#asv-general-text	TW @AppSec_Village YT AppSec Village
BioHacking Village	Forum	BHV Desc	#bhv-general-text	TW @DC_BHV YT Biohacking Village TI biohackingvillage
BlockChain Village	Forum	BCV Desc	#bcv-general-text	TW @BCOSvillage
Blue Team Village	Forum	BTV Desc	#btv-general-text	TW @BlueTeamVillage TI BlueTeamVillage
Car Hacking Village	Forum	CHV Desc	#chv-welcome-text	TW @CarHackVillage
Career Hacking Village	Forum	CRV Desc	#cahv-general-text	TW @HackingCareer
Cloud Village	Forum	CSV Desc	#cloudv-general-text	TW @cloudvillage_dc
Crypto and Privacy Village	Forum	CPV Desc	#cpv-general-text	TW @CryptoVillage TI cryptovillage SL cryptovillage YT Crypto and Privacy Village
Data Duplication Village	Forum	DDV Desc	#ddv-general-text	TW @DDV_DC
Ethics Village	Forum	ETV Desc	#ev-general-text	TW @EthicsVillage
Hack The Sea	Forum	HSV Desc	#htsv-general-text	TW @hack_the_sea
Ham Exams	Forum	HRV Desc	#ham-general-text	@DC_Ham_Exams
Ham Radio Village	Forum	HRV Desc	#ham-general-text	TW @HamRadioVillage TI hamradiovillage

Village Name	Forum Link	DC Village Desc	Discord Chan	Soc Media Links
Hardware Hacking Village Solder Skills Village	Forum	HHV Desc	#hhv-infoboost-text	TW @DC_HHV
ICS Village	Forum	ICS Desc	#ics-general-text	TW @ICS_Village YT ICS Village TI ics_village
IoT Village	Forum	IOT Desc	#iotv-general-text	TW @IOTvillage TW @ISEsecurity TW @Villageidiotlab TI iotvillage
Lock Bypass Village	Forum	LBV Desc	#lbv-social-text	TW @bypassvillage
Lockpick Village	Forum	LPV Desc	#lpv-general-text	TW @tool TI tool_us
Monero Village	Forum	MOV Desc	#mv-general-text	TW @MoneroVillage TI MoneroVillage YT Monero Community Workgroup
Password Village	Forum	PWDV Desc	#pwdv-general-text	
Payment Village	Forum	PAYV Desc	#pay-labs-text	TW @paymentvillage YT Payment Village TI paymentvillage
Packet Hacking Village	Forum	PHV Desc	#phv-infoboost-text	TW @WallOfSheep FB @WallOfSheep
Recon Village	Forum	RCV Desc	#rv-general-text	TW @ReConVillage FB @ReConVillage
Red Team Village	Forum	RTV Desc	#rtv-briefings-text	TW @VillageRedTeam YT Red Team Village TI redteamvillage DC Red Team Village
Rogues Village	Forum	RGV Desc	#rov-announcements-text	TW @RoguesVillage TI RoguesVillage
Social Engineering Village	Forum	SEV Desc	#sev-general-text	TW @HumanHacker FB SocialEngineerInc
Voting Machine Village	Forum	VMV Desc	#vmhv-general-text	TW @VotingVillageDC
Wireless Village	Forum	WLV Desc	#wv-general-text	TW @WiFi_Village DC Wireless Village

Other Interesting Links

Other cons during #SummerHackerCamp

Blackhat	T @BlackHatEvents	FB Black Hat Events
BSides Las Vegas	T @BSidesLV	
r00tz Asylum	T @r00tzasylum	
Queercon	T @Queercon	FB @queercon
The Diana Initiative	T @Dianainitiative	FB @dianainitiative

#DEFCONSAFEMODE #BadgeLife Tracker

Guides/Tips/FAQs

[Lonely Hackers Club - DEF CON n00b guide - reddit thread](#)

[DEF CON for N00bs](#)

[The Lost Policymaker's Guide to Hacker Summer Camp](#)

[Preparing for "Hacker Summer Camp"](#)

[General / previous years](#)

[JK-47 - BSidesLV & DEFCON Conference Tips](#)

[Just another DEF CON guide](#)

[HACKER SUMMER CAMP 2018 GUIDE](#)

[On Attending DefCon](#)
