



WELCOME TO DEF CON 26

What if you could go back in time to 1983, frighteningly close to George Orwell's 1984? It would be a year before full control of information, dis-information, false history narratives, your loss of personal agency and identity. As a hacker, researcher, artist or academic, what would you do to try and prevent this? That thought inspired the theme of DEF CON this year. It's not '84 yet, but it feels like we are getting awfully close. What will you do?

This will be our second and final year here. The biggest change for us is our outgrowing Caesars Palace and expanding to the Flamingo and Linq hotels. What happens when we finally out-grew the big convention spaces in one property? It is something I have thought and worried about for a number of years. Do you cap attendance and do on-line registration, or find a way to grow for everyone that wants to attend? Each has risks.

I went with growth for everyone, and that means new space so we could add new villages, workshops, parties, and events that we simply didn't have space for last year. We are letting fresh villages in to try something new and take risks, expanding the workshops, and even having a pool for evening parties again at the Flamingo!

We purchased all new DC TV gear to expand our speaking tracks to six hotels, and have been working hard to record as much content as possible. I'm a believer in the "If you didn't record it then it didn't happen" philosophy, with people all over the world wishing they could be here and I want to share our content with them.

A conference this big can't happen without the help of hundreds of Goons, speakers, village organizers, artists, work shop trainers, demo labs creators, CTF teams, party planners, and more. At last count almost 1,600 people are involved in throwing this party. I'd like to thank them for helping build DEF CON, and thank you for attending!

The Dark Tangent

UNDERGROUND NETWORK

NETWORK INSTRUCTIONS:===== DCTV RETURNS!

The DEF CON NOC delivers the cyberz throughout the different properties the conference is held.

If you want to get online, remember there are two (and only two) official ESSIDs you should use to access the intertubes:

The encrypted one with 802.1x authentication and digital certificate verification (DefCon) and the unencrypted, wild-west of the wireless networks (DefCon-Open). Please choose wisely.

Despite the fact that the 802.1x Godz seemed to have smiled at us for the past couple of years, never forget we're talking about the Wi-Fiz: where radio wavez make packets fly and digital voodoo makes the communications secure, dodging the blockchains and those pineapples along the way.

We test stuff before we go onsite, but things might change on how all operating systems, drivers and users deal with the Wi-Fiz. There are might be some devices out there that really do not like 802.1x with PEAP authentication. In particular, for quite a while some Android platforms wouldn't verify the RADIUS server certificate prior to sending the user's credentials to enter the network. And this is not cool.

And, choosing for the device to "not verify server certificate" will probably not only let that device connect to one of the hundreds of rogue access points on the show floor but will also send your login credentials to a rogue radius server. This is also a bad thing.

Because of these, and a bunch more cyber common sense (™) reasons, do not, I repeat, do NOT choose the same credentials (aka: username and password) used for your important stuffz, like shopping sites, online-banking, the pornz, your windows domains (yeah, it happened before) to connect to the hacker conference network.

For updated information and instructions on how to connect to the Wi-Fi with the n0t-s0-1337 Operating Systems along with the link to download the digital certificate to be used, visit <https://wifireg.defcon.org>. And if you don't know how to properly configure the Wi-Fiz on your üb3r-1337 linux distro, you should consider a new platform.

For other NOC updates visit <https://www.defconnetworking.org> and also

follow us on the twitterz @DEFCON_NOC

This time we are broadcasting live to the Hotel TVs again! This year we will be in six hotels on the strip! For more information on TV Channels & links to the live streams visit DCTV.defcon.org. Please also check twitter @DEFCON_TV for info about our feeds or feedback for our team.

We are planning to have the DCTV talks on the in-room TVs in the following properties this year:

Caesars, Paris, Ballys, Flamingo, Linq, and Harrahs.

Do note that Flamingo, Linq, and Harrahs are new for us this year, and we may run into unforeseen issues, but will work as hard as we can to get all six properties on-line for your viewing pleasure.

THE DEF CON MEDIA SERVER IS BACK AGAIN!

<https://10.0.0.16/> or

<https://dc26-media.defcon.org/>

Browse and leech files from all the past DEF CON conferences and find this year's presentation materials, white papers, slides, etc.

Since last year the DEF CON collection has been updated as well as many more hacking conferences added to the infocon.org collection.

We expect you to leech at full speed, and the server is warmed up and ready to go. Enjoy!

To make things easier for you here are some example wget commands and TLS certificate information:

The dc26-media.defcon.org TLS certificate fingerprint:

Serial Number:
0250E3021BFB8B91D364BB71F739B71D

(SHA256) DCE6 CEC3 4CE7 DAA2 D998 9151
D6DA C549 40F8 D841

EXAMPLE wget command to download all of DEF CON 25:

wget -np -m "https://dc26-media.defcon.org/infocon.org/cons/DEF CON/DEF CON 25/"

THE BADGE

The year is 1983. The state of humanity as we know it rests on the precipice of an Orwellian collapse!

Or does it?

If we were to graph out the cultural health of a society, we might think to create a drastic cliff coinciding with the events captured in George Orwell's 1984. We might even say that as a people, we would obviously never allow our values to become controlled by paranoia, fear, and Big Brother.

Reality, however, is much less dramatic. Societal values develop from the little details, the decisions made by individuals on a day to day basis, and

minute changes we allow ourselves to accept. It is in these seemingly inconsequential concessions that we choose to either be part of the solution or contribute to a dystopian future. Food for thought: Everyone is branding web cam covers for your laptop.

With that inspiring message, we present this year's Defcon 26 badge created by the Tymkrs! Each badge consists of an interactive web of decisions you need to make which not only define what "kind of hacker" you are but also impacts and changes the individuals you associate with. The overall design aesthetic of the badge highlights that the hacker community

is found all over the world – from the hacker soldering wires in a garage to the researcher studying neural networks in a research institute. We also wanted to acknowledge that the hacker community encompasses more than those with programming or hardware hacking skills, it also includes the teachers, artists, and journalists. Welcome to DEFCON City:

- Humans – White Soldermask/Black Silkscreen = Garage
- Contest – Yellow Soldermask/Black Silkscreen = Library
- Goon – Red Soldermask/White Silkscreen = Prison
- Artist – White Soldermask/Blue Silkscreen = Gallery
- Press – Green Soldermask/White Silkscreen = Broadcast Station
- Vendor – Purple Soldermask/White Silkscreen = Factory
- Speaker – Blue Soldermask/White Silkscreen = Theater
- Call for Papers (CFP) – Orange Soldermask/White Silkscreen = School

Each badge's story is simple to interface with via the direction pad and + / - buttons. Your character is highlighted in green and depending on your decisions, you can move to new rooms, gain different clues, and open closed doors. Interacting with others from different groups will also help you as you work towards being the best hacker you can be. But be careful, depending on what kind of hacker you are, the red guard that roves around the same board may be your friend, or enemy. Additional clues can be found if you plug the badge in, and yet even more if you can gain control of various elements of the badge.

The balance of what kind of hacker you are is reflected in the DEFCON logo between Red and Green lights. Each choice that contributes to a dystopian future will be reflected in Red, and each choice that helps future hackers will be reflected in Green.

Here's to a greener future! Enjoy the DEFCON 26 Badge!

GOONS

DEF CON Goons are the electrons that enable the conference to run, and should you have a question or need help they are there for you. Here are some goon facts:

New for DEF CON 26 Goons should all have visible patches with their nickname on them so it is easier to remember who you talk to about what.

Goons are in one of two states, either ON duty or OFF duty.

If they are ON DUTY they will be wearing a current year, red, DEF CON 26 Goon shirt, a current year Goon badge, and a name patch.

If Goons are OFF DUTY they will not be wearing the red Goon shirt, but may still have a Goon badge on so they can still access the meeting spaces.

Goons ON DUTY are not supposed to drink alcohol.

Goons OFF DUTY have been known to drink alcohol.

PAST Goons may seen wearing previous red shirts or badges as they helped run a past DEF CON, but that DOES NOT make them a current DEF CON 26 Goon.

On almost all the Goon shirts there is a department name on the back to tell you what department you are talking with. Please use this and the name patch if you have any feedback on Goons, good or bad. Feedback can be sent to feedback@defcon.org

Goons Goon for many reasons, but the pay isn't one of them. They put in long hours and many weeks or months of planning and take time off work to make the con happen for everyone. Please feel free to ask them questions if you have any desire to join the ranks at a future Con.

Goon Name



CONFERENCE CODE OF CONDUCT

Last updated 3.6.15

DEF CON provides a forum for open discussion between participants, where radical viewpoints are welcome and a high degree of skepticism is expected. However, insulting or harassing other participants is unacceptable. We want DEF CON to be a safe and productive environment for everyone. It's not about what you look like but what's in your mind and how you present yourself that counts at DEF CON.

We do not condone harassment against any participant, for any reason. Harassment includes deliberate intimidation and targeting individuals in a manner that makes them feel uncomfortable, unwelcome, or afraid.

Participants asked to stop any harassing behavior are expected to comply immediately. We reserve the right to respond to harassment in the manner we deem appropriate, including but not limited to expulsion without refund and referral to the relevant authorities.

This Code of Conduct applies to everyone participating at DEF CON - from attendees and exhibitors to speakers, press, volunteers, and Goons.

Anyone can report harassment. If you are being harassed, notice that someone else is being harassed, or have any other concerns, you can contact a Goon, go to the registration desk, or info booth.

Conference staff will be happy to help participants contact hotel security, local law enforcement, or otherwise assist those experiencing harassment to feel safe for the duration of DEF CON.

Remember: The CON is what you make of it, and as a community we can create a great experience for everyone.

- The Dark Tangent



DEF CON SUPPORT HOTLINE

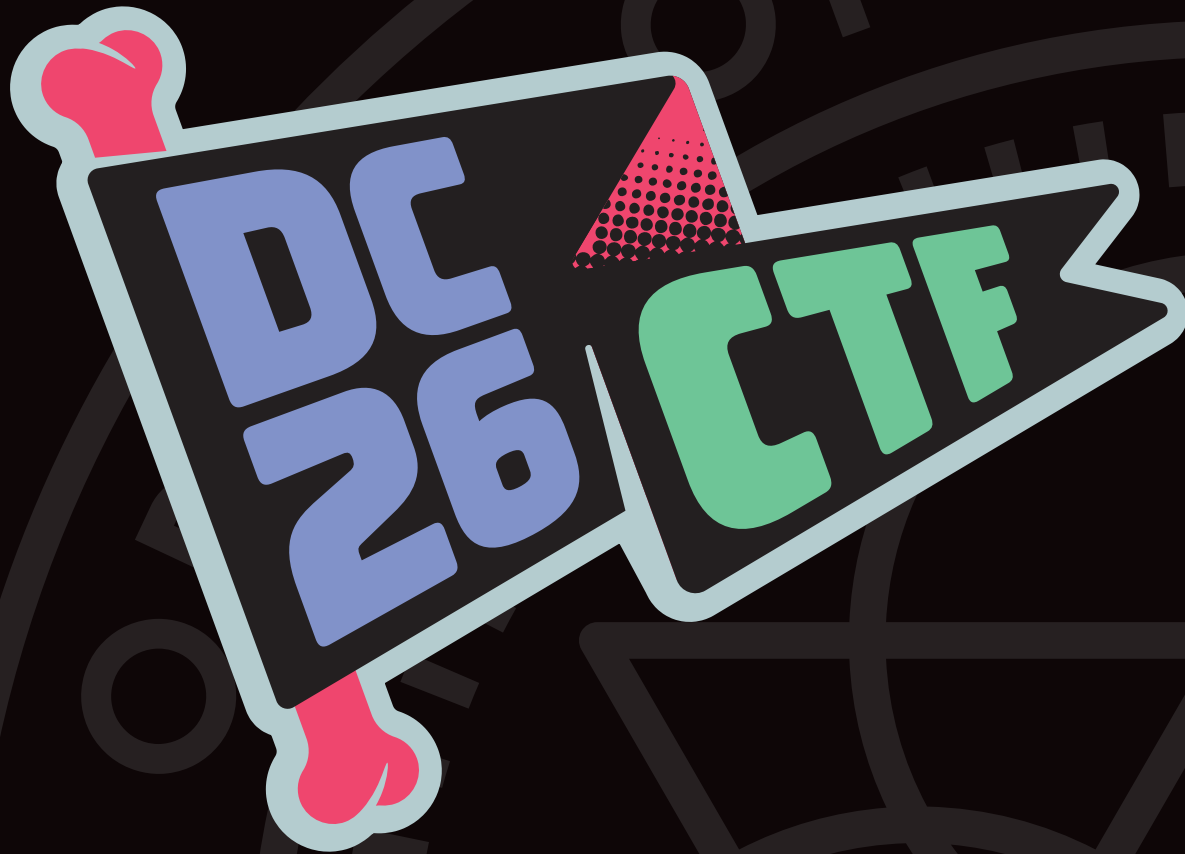
Sometimes you may not want to contact a Goon at the Info Booth or walking around in person with a problem, and so this year we have added a phone option to tell us about concerns.

You can reach DEF CON staff during normal hours of operation (8am to 4am) to anonymously report any behavior violating our code of conduct or to find an empathic ear by calling +1 (725) 867-7255.

For relevant issues, we are collaborating with several organizations including Kick at Darkness, The Rape Crisis Center Las Vegas, and the Nevada Coalition to End Domestic and Sexual Violence to provide expert resources for survivors, including dedicated support for LGBTQ+.

CAPTURE THE FLAG

AT DEF CON 26



WELCOME TO DEF CON CTF 26, A NEW ORDER FOR A NEW ERA.

For decades, upstanding cybercitizens suffered the chaos of unchecked security vulnerabilities, shamelessly encouraged by the regimes of goons (DC4 – DC9), ghettohackers (DC10 – DC12), kenshoto (DC13 – DC16), ddtek (DC17 – DC20), and legitbs (DC21 – DC25). The time has come for a new era. An era of security. An era of obedience. An era of order: the Order of the Overflow.

Cybercitizens, rejoice: software security vulnerabilities are no more! On this auspicious day, the 1st of August, 1983, the Order of the Overflow has decreed that it is illegal to discover or exploit security vulnerabilities. No longer will the compliant

cybercitizens of the world be held hostage by malicious hackers, who exploit vulnerabilities to enrich themselves with ill-begotten flags. These parasites on society forcefully take time and effort away from developing software that enhances and improves your lives. There is no room for them in the orderly new world.

This year, the world's most skilled cybercitizens gather together and obediently work toward a new, harmoniously monotonous future. There will be no hacking, no stealing of flags, and no victors. You will obey.

Order through control. Order Over Overflows.

CAPTURE THE FLAG?

Capture the Flag is a hacking competition in which teams to compete out-hack each other. Originating over two decades ago at DEF CON 4, CTF has now grown to become a global phenomenon. CTFs are held every weekend, and teams join online or fly around the world to test their skills.

Traditionally, DEF CON CTF has been an “attack/defense” CTF: teams are provided identical sets of network services, and must defend their instances of these programs while exploiting vulnerabilities in the instances run by their opponents. That being said, each organizer has leeway to shape the game to their vision. This year, we have introduced a twist on the format, and will continue to tinker and experiment throughout our tenure.

Only the top teams in the world are invited to DEF CON. Teams qualify by performing well in the DEF CON Qualifier event (held online in May), by winning a number of other prominent Capture the Flag competitions, or, of course, by winning last-year's DEF CON CTF.

This year, we have gathered the world's top 24 teams. The teams are:

Odaysober
A*0*E
BFS
binja
C.G.K.S
DEFKOR00T
Dragon Sector
HITCON
hxp
KaisHack+PLUS+GoN
koreanbadass
mhackeroni
pasten
PPP
PwnThyBytes
r3kapig
RPISEC
Samurai
Sauercloud
Shellphish
Spaceballs
Tea Deliverers
TeamBaguette
TokyoWesterns

Come watch them hack in the CTF room. One day, you may take their place. Or ours.

WHO IS THE ORDER OF THE OVERFLOW?

We have been here for a while. We wandered the halls in awe of the master hackers at DEF CON 9. We spent sleepless nights competing against them every year since DEF CON 12. We have been the hackers, and we have been the hacked. Now, as the new organizers of DEF CON CTF, we hope to shepherd the game through the next generation of technological and societal shifts. Just as importantly, we will keep DEF CON CTF a spectacle that can be used to inspire the next generation, who, just like we used to do, will first wander the halls in awe of the players and then hack them to shreds a decade later.

RESOURCES

The following resources may be helpful to interested hackers!

Our philosophy: <https://www.ooverflow.io/philosophy.html>

Game announcements: <https://twitter.com/ooverflow>

DEF CON CTF scoreboard: <https://ctf.ooverflow.io>

CTF tracker: <https://ctftime.org>



PARTY MUSIC

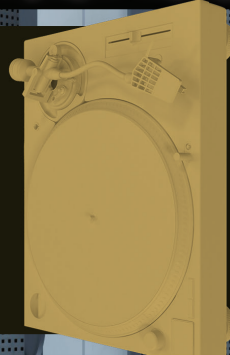
THURSDAY



2100 - 2200	YURKMEISTER
2200 - 2300	OS. SYSTEM
2300 - 0000	ICETRE NORMAL
0000 - 0100	DJ 427
0100 - 0200	ACID-T
0200 - 0300	TINEH NIMJEH

2100 - 2200
2200 - 2245
2245 - 2330
2330 - 0015
0015 - 0115
0115 - 0215
0215 - 0300

JG & THE ROBOTS
YT CRACKER
DUALCORE
MC FRONTALOT
TBD
SCOTCH & BUBBLES
CIRCUIT STATIC



FRIDAY

SATURDAY



2130 - 2230	SKITTISH & BUS
2200 - 2300	ZEEDLER ENCANTI
2330 - 0100	JUNO REACTOR
0100 - 0200	MISS JACKALOPE
0200 - 0300	STAR73FARM

DANCE WITH US

WHILE PLEASURE IS STILL LEGAL

MAIN ROOM
ALL NIGHT

PARTIES & MEETUPS

303 PARTY

What can one say but "303 Party" to let you know where the mayhem will be? Join the members of the 303 organization as they redefine pool party with their own music, entertainment, and mile high shenanigans! A repeat favorite of DEF CON attendees, with DJ's from across the community as well as creative works and technical expertise. What can we say, it's 303!

Friday Location: Virginia City, Flamingo

Saturday Location: Pool, Flamingo

Time: 20:30

ARCADE PARTY

Relive once again the experience of the arcade. From classics to a custom built 16 player foosball table! Grimm & Scythe bring back a favorite as you jam out a DJ battle while taking another swipe at that high score on your favorite classic video games. No quarters required!

Location: Mesquite, Flamingo

Time: 20:30 Friday

BLANKETFORTCON

Check your ego at the door, grab some building materials and join in the celebration of the creativity and originality that is the pillow fort! A host of DJs will be spinning from a pirate ship as you share and create your own unique environment. All aboard!

Location: Carson City, Flamingo

Time: 20:30 Saturday

GEEKPWN

Part contest, part open discussion of security, part talent show and 100% fun! Join the folks from GEEKPWN for an evening of entertainment with a focus on information security from China. Expect contests, serious discussion, music, and an environment open to your ideas.

Location: Scenic, Flamingo

Time: 20:30 Friday

HACKER KARAOKE

Two great things that go great together! Join the fun as your fellow hackers make their way through songs from every era and style. Everyone has a voice and this is your opportunity to show it off! Quickly becoming a DEF CON tradition and a favorite of people from all skill levels.

Location: Chillout Lounge, Caesars

Palace Emperors ballroom

Time: Friday 2000-0200, Saturday 2000-0200

HOUSE OF KENZO

Come celebrate the culture of DIY or die! The future has not been written yet so come and mingle with the authors of the time to come and celebrate creating a culture of global communication and culture. Live music and open minds will meet your ideas and help you trailblazer the next century.

Location: Twilight, Flamingo

Time: 20:30 Friday

LIVE BAND KARAOKE

Think you have karaoke chops? Kick it up to the next level by performing your favorite songs with a live band! The band with the

best name ever, DON'T PANIC provides the music and you provide the vocal talent. You won't need an electronic thumb or the help of the Dentrasi to get into this party, just bring yourself and your towel.

Location: Vista, Flamingo

Time: 21:00 Friday

LONELY HACKERS CLUB

If only Sergeant Pepper had owned a Commodore 64! Come meet the people you communicate with on a daily basis in person as you dance and chat the night away. Just keep in mind that this IS Las Vegas and when you wake up in the morning those marriage certificates are still binding!

Location: Eldorado Ballroom, Flamingo

Time: 20:30 Saturday

SECK THE WORLD

A Tiki themed gathering of the people who make up seckc.org. Come get a taste of this slice of hacker culture as you party the night away. The hotel won't let us have Tiki torches so grab some glow-sticks and bamboo and help the theme while live DJs keep your feet moving.

Location: Mesquite, Flamingo

Time: 20:30 Saturday

WIRELESS VILLAGE

Join the folks from the wireless village in an informal party atmosphere and celebrate all the works that they do to make DEF CON awesome. This is your moment to make new friends, reunite with old ones, and celebrate the wireless lifestyle. Live music and social interaction await you, along with some of the thought leaders and presenters in the realm of wireless communications.

Location: Wireless Village

Time: TBA (Visit the Wireless Village)

VET CON

A party thrown by Veterans for everyone! Come join in as veterans from all branches come together to celebrate and take on challenges that you only hear about in movies. Space force recruiting? Airmen in a chair race? Military drill displays? All this and more. It's time to raise hell the way our people in uniform are famous for.

Location: Savoy, Flamingo

Time: 20:30 Friday

MEETUPS

BRUCAMP

A play within a play, this meetup is for conference organizers to come together and share their best ideas, tips and methods of running their cons in a social environment. The goal is to help improve the conference experiences for all and to help take away some of the headaches in running a con. A great gathering for con organization veterans as well as anyone looking to start their own con.

Location: Livorno, Caesars Palace

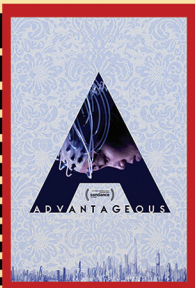
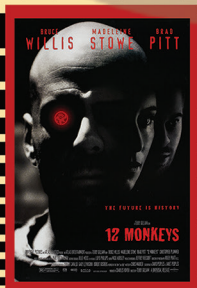
Time: 16:00 to 18:00, Thursday

#DCGOTHCON

We want a flashmob to get all the goths in one spot. To make friends! To get dressed up! Find out more info via @clevercat and follow #DCgothcon

MOVIE NIGHT

WE ARE WATCHING



FRIDAY

12 MONKEYS

TERRY GILLIAM, TIME TRAVEL, SUPERVIRUS

CGC DOCUMENTARY

ROBOTS VS. ROBOTS AT DC 24

ALPHAVILLE

60s FRENCH TECHNO-NOIR

8PM, TRACK 2

SATURDAY

1984

THE GOOD VERSION THEY DONT SELL ANYMORE

ADVANTAGEOUS

HOPEFUL DYSTOPIA

CHILDREN OF MEN

FIGHT FOR THE FUTURE

BONUS MOVIES

INSIDE THE FAKE SCIENCE FACTORY

HOW PROFITABLE BOGUS SCIENCE GETS MADE
SATURDAY AT 16:00 IN TRACK 3

REVERSE ENGINEERING

TEASER FOR DOC SERIES - SEE THE TALK FRIDAY
17:00, TRACK 3 - NIRENBURG AND BUCHWALD

PARTIES & MEETUPS

Location: TBA Flashmob

Time: TBA

/R/DEF CON MEETUP

Do you participate in the DEF CON subreddit? This meetup is for you! A gathering of the denizens of /r/DEF CON while at DEF CON to mingle and meet face to face. Newcomers and veterans alike are welcome to meet and greet while sharing the DEF CON experience.

Time: 20:30 Friday

Location: Chillout Lounge, Laughlin, Flamingo

FRIENDS OF BILL W MEETING

Times: Thursday the 9th: 12 noon and 5 pm, Friday the 10th 12 noon and 5 pm, Saturday the 11th 12 noon and 5 pm, Sunday the 12th at 12 noon.

Location: Behind DCIB IN OFFICE 4

HACKER FLAIRGROUNDS

This is the meetup destination for badge collectors, designers, and prototypers that you have been waiting for! A social environment to show off you custom badges,

discuss projects to make you own badges and to talk to collectors who cherish your work. Flashing LEDs, crafting time, trading, and the celebration of badge craft all in one.

Location: Chillout Lounge, Laughlin, Flamingo

Time: 20:30 Saturday

HACKING FOR SPECIAL NEEDS

A meetup for parents of children and individuals with special needs within the DEF CON community. The meeting is not only social but also a exchange of information and helpful tips to help improve the lives of families and individuals and to celebrate their place in the DEF CON community.

Time: 17:00 to 19:00, Thursday

Location: Anzio, Caesars Palace

LAWYER MEET

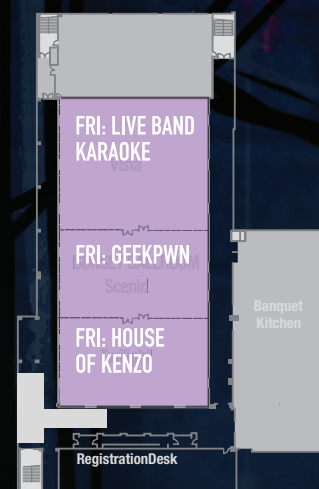
If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join your host Jeff McNamara at 18:00 on Friday, August 10th, for a friendly get-together, followed by dinner/drinks and conversation.

Location: Carson City, Flamingo

Time: Friday 19:00

FLAMINGO LAS VEGAS

DEF CON 26 Nocturnal Arrangement



THE FLAMINGO POOLS

VISIT THE POOLS EVERY NIGHT!

LIVE DJ'S

MULTIPLE POOLS

VARIOUS HOSTED PARTIES

LIFEGUARDS ON DUTY

REBELLIONS TO PLAN

NIGHTTIME EVENTS@ CAESARS

HACKER KARAOKE - CHILLOUT (EMPEROR'S BALLROOM)

MOVIE NIGHT - TRACK 2 (OCTAVIUS BALLROOM)

HACKER JEOPARDY - TRACK 3 (FORUM BALLROOM)

WHOSE SLIDE IS IT ANYWAY? - CONTEST AREA STAGE (AUGUSTUS BALLROOM)

DRUNK HACKER HISTORY - CONTEST AREA STAGE (AUGUSTUS BALLROOM)

DEF CON MUSIC EVENTS - TRACK 1 (PALACE BALLROOM)

CORPORATE CONVENTION CENTER THIRD FLOOR



VILLAGES



IOT VILLAGE

Friday: 10:00 to 19:00,
Saturday: 10:00 to 19:00,
Sunday: 10:00 to 13:00
Location: Turin Verona
Trevi - Caesars

Organized by security consulting and research firm Independent Security Evaluators (ISE), IoT Village delivers advocacy for and expertise on security advancements in Internet of Things devices.

IoT Village hosts talks by expert security researchers who dissect real-world exploits and vulnerabilities and hacking contests consisting of off-the-shelf IoT devices. IoT Village's contests are brought to you by SOHOpelessly Broken™, the first-ever router hacking contest at DEF CON. The ISE research that inspired the SOHOpelessly Broken™ contests delivered 56 CVEs to the infosec community. Over the years at DEF CON, IoT Village has served as the platform to showcase and uncover nearly 219 new vulnerabilities in connected devices.

Follow both ISE (@ISEsecurity) and IoT Village (@IoTville) on Twitter for updates on talks, contests, and giveaways. Organized by security consulting and research firm Independent Security Evaluators (ISE), IoT Village delivers advocacy for and expertise on security advancements in Internet of Things devices.

IoT Village hosts talks by expert security researchers who dissect real-world exploits and vulnerabilities and hacking contests consisting of off-the-shelf IoT devices. IoT Village's contests are brought to you by SOHOpelessly Broken™, the first-ever router hacking contest at DEF CON. The ISE research that inspired the SOHOpelessly Broken™ contests delivered 56 CVEs to the infosec community. Over the years at DEF CON, IoT Village has served as the platform to showcase and uncover nearly 219 new vulnerabilities in connected devices.

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

Village Schedule: https://www.iotvillage.org/#dc26_schedule
Website: <https://www.iotvillage.org>
Twitter: @ISEsecurity, @IoTville

BIOHACKING VILLAGE

Friday: 10:00 to 20:00,
Saturday: 10:00 to 20:00,
Sunday: 10:00 - 14:00
Location: Siena Pisa
Palermo - Caesars

The Medical Industry is one of the last to be touched by technology. We have placed doctors and the study of medicine on an altar for years; the time of ivory towers, pedestals, and information isolation has come to an end. Biohackers are working on projects that have traditionally been kept in the labs of the medical institutions. We are moving science forward by working on DIY projects that matter and use citizen science to solve the economic

problems that are caused by privatizing medicine and the resources for research. Our goal is to extend beyond the scope of mission driven technology. This event and the community behind it place a strong emphasis on diversity, inclusiveness, education, collaboration, and contribution. The BioHacking Village is also focused on helping developers learn the skills and other factors associated with successful careers in biotechnology and software development. The event aims to provide opportunities to interact with like-minded scientists and developers, to learn from one another, as well as help each other see opportunities that may be available.

Village Schedule: <http://villageb.io>
Website: villageb.io
Twitter: @dc_bhv



CRYPTO + PRIVACY
VILLAGE

CRYPTO & PRIVACY VILLAGE

Friday: 10:00 to 18:30,
Saturday: 10:00 to 18:30,
Sunday: 10:00 to 14:00
Location: Milano
II - Caesars

At the Crypto & Privacy Village you can learn how to secure your own systems while also picking up some tips and tricks on how to break classical and modern encryption. The CPV features talks on a wide range of crypto and privacy topics, including GDPR, domain fronting, and privacy education, from experts. We'll also have an intro to crypto talk for beginners, and some crypto-related games and puzzles. Come check it out! @cryptovillage www.cryptovillage.org

Village Schedule: <http://www.cryptovillage.org/dc26>
Website: www.cryptovillage.org
Twitter: @cryptovillage



WIRELESS VILLAGE

Friday: 10:00 to 18:00,
Saturday: 10:00 to 18:00,
Sunday: 10:00 to 14:00
Location: Milano
V VI - Caesars

The Wireless Village is a group of experts in the areas of information security, WiFi, and radio communications with the common purpose to teach the exploration of these technologies. We focus on running classes on topics such as WiFi and Software Defined Radio, hosting guest speakers and panels, and providing the very best in Wireless Capture the Flag (WCTF) practice to promote learning on cutting edge topics as it relates to radio communications. <http://www.wirelessvillage.ninja/crew.html>

Speaker schedule can be found on our website: <http://www.wirelessvillage.ninja/schedule.html>

Co-located with the Wireless Village is the Wireless Capture the Flag. Come for the talks, stay for the practice and the competition. The Wireless Village is a group of experts in the areas of information security, WiFi, and radio communications with the common purpose to teach the

exploration of these technologies. We focus on running classes on topics such as WiFi and Software Defined Radio, hosting guest speakers and panels, and providing the very best in Wireless Capture the Flag (WCTF) practice to promote learning on cutting edge topics as it relates to radio communications. <http://www.wirelessvillage.ninja/crew.html>

Speaker schedule can be found on our website: <http://www.wirelessvillage.ninja/schedule.html>

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

Village Schedule: <http://www.wirelessvillage.ninja/schedule.html>
Website: <http://www.wirelessvillage.ninja>
Twitter: @WIFI_VILLAGE



ROOTZ ASYLUM

Friday: 10:00 to 17:00,
Saturday: 10:00 to 17:00,
Sunday: 10:00 to 14:00
Location: Milano III
IV - Caesars

r00tz Asylum at DEF CON is a safe and creative space for kids to learn white-hat hacking from the leading security

researchers from around the world. Through hands-on workshops and contests, DEF CON's youngest attendees understand how to safely deploy the hacker mindset in today's increasingly digital and prone to vulnerabilities world. Only after mastering the honor code, kids learn reverse engineering, soldering, lock-picking, cryptography and how to responsibly disclose security bugs. r00tz's mission is to empower the next generation of technologists and inventors to make the future of our digital world safer.

Village Schedule: <https://r00tz.org/2018-schedule>
Website: <https://r00tz.org/>
Twitter: @r00tzasylum

LOCKPICKING VILLAGE



Friday: 10:00 to 18:00, Saturday: 10:00 to 18:00,
Sunday: 10:00 to 13:00
Location: Forum BR 24- Caesars

Want to tinker with locks and tools the likes of which you've only seen in movies featuring police, spies, and secret agents? Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

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

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

Website: <https://toool.us/>
Twitter: <https://twitter.com/toool>



HARDWARE HACKING VILLAGE

Friday: 10:00 to 19:00,
Saturday: 10:00 to 19:00,
Sunday: 10:00 to 13:00
Location: Forum Ballroom
17-21 - Caesars

Join us for another DEF CON adventure! After 10 years of

providing a space to explore and learn about hardware, we're rebooting to bring you more hardware hacking awesomeness.

We are sharing a (very) large space with the new Soldering Skills Village, and the Badge Maker's Community Area. This puts all of your hardware hacking/making resources in one place.

For more details on hours and other events, see dchhv.org. Join us for another DEF CON adventure! After 10 years of providing a space to explore and learn about hardware, we're rebooting to bring you more hardware hacking awesomeness.

We are sharing a (very) large space with the new Soldering Skills Village, and the Badge Maker's Community Area. This puts all of your hardware hacking/making resources in one place.

For more details on hours and other events, see dchhv.org.
Website: www.dchhv.org

SOCIAL ENGINEER VILLAGE



Thursday: 10:00 to 17:00, Friday: 10:00 to 18:00,
Saturday: 10:00 to 18:00, Sunday: 10:00 to 14:00

Location: Octavius 3 - 8 - Caesars

Established at DEF CON 18 the SE Village has been the one-stop shop for all things social engineering at DEF CON. From our humble beginnings with a small room and our sound proof booth to now running 5 events and a "Human Track" where top quality and hand chosen social engineering talks are given.

The SE Village is the place for not only our flag ship event, the Social-Engineer Capture the Flag (The SECTF), but also Mission SE Impossible, the SECTF4Kids and the SECTF4Teens!

For more information and a live scoreboard of events see: <https://www.social-engineer.org/sevillage-def-con/Established>

VILLAGES

at DEF CON 18 the SE Village has been the one-stop shop for all things social engineering at DEF CON. From our humble beginnings with a small room and our sound proof booth to now running 5 events and a "Human Track" where top quality and hand chosen social engineering talks are given.

The SE Village is the place for not only our flag ship event, the Social-Engineer Capture The Flag (The SECTF), but also Mission SE Impossible, the SECTF4Kids and the SECTF4Teens!

For more information and a live scoreboard of events see: <https://www.social-engineer.org/sevillage-def-con/>

Website: <https://www.social-engineer.org>

TAMPER EVIDENT VILLAGE

Friday: 10:00 to 18:00, Saturday: 10:00 to 18:00, Sunday: 10:00 to 14:00
Location: Forum BR 24- Caesars

Defcon 26 will have the sixth annual Tamper-Evident Village! Since Decon 21, the MFP group has hosted the TEV to help Defcon attendees learn about these security technologies. Tamper is a great hobby and one of the relatively unexplored areas of physical security. Come learn about it in a friendly, hands-on environment!

What does Tamper-Evident mean?

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

What's there to do at the village?

- For your viewing pleasure, collections of high-security tamper-evident seals from around the world.
- Sit-down presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.
- Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags.

• Electronics rework & reverse engineering stations for working with electronic tamper seals.

• Contest workspaces (space permitting). Sit down in the village and work on your tamper contest box! The village should have a variety of tools you can use to help defeat your box.

• Counterfeiting! Learn about techniques used to counterfeit documents, identification cards, and much more!

Contests hosted in the Tamper Village:

- Tamper-Evident King of the Hill Contest; a full-featured tamper challenge! Instead of the weekend-long contest we're hosting a King of the Hill format where

you tamper single items at your leisure and attempt to beat the current best. There can be only ONE! No sign ups required, play on-site when the TEV begins.

- The Box; an electronic tamper challenge. An extremely realistic explosive with traps, alarms, and a timer ticking down. One mistake and BOOM, you're dead. Make every second count! Sign ups on-site when the TEV begins.

- Badge Counterfeiting Contest; submit your best forgery of a Defcon human badge. Other target badges are also available for those looking for more counterfeit fun!



DATA DUPLICATION VILLAGE

Thursday: 16:00 to 19:00, Friday: 10:00 to 17:00, Saturday: 10:00 to 17:00, Sunday: 10:00 to 11:00
Location: Capri - Caesars

We provide a "free-to-you" service of simply handing you terabytes of useful data. Want data? Just hand us drives. Drives should be 6TB SATA 512byte sector (512e) 7200 RPM. For a full set of data you

will need three drives, and they take over 14 hours to copy.

Two of the drives make up the rainbow table and password hash data set, and the third drive is a mirror of infocon.org and all DEF CON materials including cons, podcasts, and documentaries.

This year we're also having scheduled talks on Friday/ Saturday about drive duplication (why/how), drive forensics, data backups, data recovery, data management on SSDs vs. HDs, and other related topics!

Schedule and updates to be posted at dcdv.org.

This year, we will be in the Capri room at Caesars and plan to be open for the following hours:

Thursday, August 9th 4:00pm - 7:00pm

Friday, August 10th 10:00am - 5:00pm

Saturday, August 11th 10:00am - 5:00pm

Sunday, August 12th 10:00am - 11:00am (last chance pickup)



DEAF CON

Friday: 10:00 to 17:00,
Saturday: 10:00 to 17:00,
Sunday: 10:00 to 14:00
Location: Patrician - Caesars

DEAF CON is a California 501 (c)(3) Non-profit organization.

We provide outreach to the Deaf and HH community and information security community. We encourage Deaf and HH information security professionals to attend conferences,

like Defcon. We help to provide communication services and spaces for professionals to meet and network with others. Anyone can come and attend our meet up and hangout!

DEAFCON Meet Up: The event itself will take place on Saturday at Noon in the Chillout Lounge.

Interpreters: The interpreters will work two shifts throughout the conference. We will have interpreters working day and night shifts throughout Defcon. The exact times and locations will be posted via Twitter.

Website: www.deafconinc.org

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

RECON VILLAGE

Friday: 1200 - 1840, Saturday: 1000 - 1840, Sunday: 1000-1300
Location: Florentine I II - Caesars

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, CTFs, etc. with a common focus on Reconnaissance. The core objective of this village is to spread awareness about the importance of reconnaissance, open source intelligence (OSINT) and demonstrating how even a small information about a target can cause catastrophic damage to individuals and organizations.

Recon Village appeared at DEF CON 25 for the very first time and we received an overwhelming response from speakers, CTF participants, and attendees. We strive to make Recon Village even bigger this time and are expecting more active participation from the attendees.

We will also be running a Jeopardy Style OSINT CTF Contest throughout the Village. We plan to make the CTF more challenging this year. The challenges will typically revolve around harvesting information about target organizations, their employee's social media profiles, their public svn/gits, password breach dumps, darknet, paste(s) etc. followed by active exploitation of virtual targets. All the target organizations, employees, servers, etc. will be created by our team and hence will not attract any legal issues.

There will be awesome rewards for CTF winners, along with free t-shirts, stickers, village coins, and other schwag which attendees can grab and show off.

Village Schedule: <http://reconvillage.org/schedule/>

Website: <http://reconvillage.org/>

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

Other: [Facebook://reconvillage](https://facebook.com/reconvillage)

SOLDERING SKILLS VILLAGE

Friday: 10:00 to 19:00, Saturday: 10:00 to 19:00, Sunday: 10:00 to 13:00
Location: Forum BR 20-21 - Caesars

The Soldering Skills Village is the soldering and badge-building arm of the Hardware Hacking Village. It provides a dedicated place for building, repairing, and modifying badges and other electronic devices. It is a place to learn and improve electronics skills as well as to pass along knowledge to others. In addition to the usual soldering stations and work areas, we will also have tables and chairs

set aside for people to congregate, collaborate, and hack the various community badges. We have a variety of parts and random hardware to include in or support hacking projects.

VOTING MACHINE HACKING VILLAGE

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

Location: Forum Ballroom 14-16, Caesars

The Voting Machine Hacking Village is back! This year we will run elections on electronic voting machines still in use across the USA - and you are welcome to hack them. We will also have new models of voting machines, some of them never-before subjected to public or independent security review.



AI VILLAGE

Thursday: N/A, Friday: 10:00 to 18:00, Saturday: 10:00 to 18:00, Sunday: 10:00 to 14:00

Location: Florentine III - Caesars

The AI Village at DEF CON is a place where experts in AI and security (or both!) can come together to learn and discuss the use and misuse of artificial intelligence in computer security. Artificial Learning techniques are rapidly being deployed in core security technologies like malware detection and network traffic analysis, but their use has also opened up a variety of new attack vectors against such systems.

Come participate in the AI-CTF, a jeopardy-style CTF with a variety of challenges suitable for participants of all experience levels, or the Pommerman contest, where you can pit your Bomberman skills against AI agents that other participants have trained to see who emerges triumphant.

We also have more than 27 talks, panels, workshops, and a series of rotating exhibits.

Village Schedule: <https://aivillage.org/events/vegas2018/>

Website: <https://aivillage.org/>

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

Other: <https://aivillage.org/events/vegas2018/>

DRONEWARZ VILLAGE

Friday: 10:00 to 18:00, Saturday: 10:00 to 18:00, Sunday: 10:00 to 14:00
Location: Abruzzi - Caesars

DroneWarz drone hacking games and challenges are designed for harnessing innovation and having fun with UAV emerging technologies. Our Village creates a Drone Hacking Arena with four (4) primary challenges each consisting of 3-4 flags/objectives.

Drone Hacking Arena - Hack drones and determine their motives - This Village arena allows teams to engage active mission and post-mission drones to intercept and control them (capture them in flight) and perform forensics on missions. For safety purposes, all drones are tethered in the arena. Our challenges include:

VILLAGES

PWN-a-DRONE - Drone Hacking Challenges - Our drone hacking challenges will be posted with commercial and non-commercial paired and operational and tethered drones in advance of the village. Find vulnerabilities and exploit them.

CONQUER the CONTROLLER - Control Hacking Challenges - Our controller hacking challenges will be posted for several commercially available drone controllers and varying levels of difficulty. Intercept paired drones in flight!

PAYLOADZ - REDSKYZ - Program Payloads for anti-jamming, controller interception, defense evasion, defense deception, and other creative applications to dominate the skyz. This is our sandbox for offensive drone applications.

MISSIONZ - BLUESKYZ - This is our defensive sandbox. These challenges allow you to engage in capture, interception, forensic discovery and threat modeling for drones captured during a mission. Teams that can capture an in mission drone and accurately determine the flight path, display surveillance images/FPV, and determine the drone's

Website: <https://dronewarz.org>



VX (CHIP-OFF) VILLAGE

Friday: 10:00 to 17:00,
Saturday: 10:00 to 17:00
Location: Tribune
- Caesars Place

VXRL is founded by a group of passionate security researchers and white-hat hackers in Hong Kong. Our team has deep expertise in software and hardware security, and we have hands-on domain knowledge in several vertical industries. Our mission is to make the cyberspace a safe place for the future.

During the chip-off village, visitors shall have an opportunity to remove the embedded emmc chip from the devices and re-solder on the small circuit board. And our experts will demonstrate how to attack the IoT/mobile devices to obtain privilege and gain access control as well as the data stored. We will also introduce some inexpensive JTAG/ISP and chip-off equipments on-site and for your testing

Village Schedule: www.dcvxv.org
Website: www.vxrl.hk
Twitter: @vxresearch
Other: hello@vxrl.hk



MOBILE MUSEUM

Friday, Saturday,
& Sunday
Location: Florentine
IV- Caesars

Atari 2600, Commodore, Intellivision, TRS-80, Apple, floppy disk, dot matrix, Colecovision, Oregon Trail, PACMAN, Donkey Kong: Were these the cutting edge gadgets of your youth? Your parents youth? Do you want to experience them again, or for the first time? This free hands on museum of retro technology will be available for use by the public. Parents will have the opportunity to show their children the technology they used

growing up and enjoy it together. Retro Technology geeks can play the games of yesteryear, and use 9600 baud modems with Vic 20s, Apple IIe, TRS-80s, and more to connect to the internet. Get your children and America's youth interested in STEM (Science, Technology, Engineering, and Math) by introducing them to the golden age of technology.

We are a free and non-profit museum that brings vintage technology products to events and conference across the country. We allow you to experience the joys of technology from the past! Visitors are free to use many of the vintage computers and gadgets in our collection. All the computers and games are in working condition and setup for visitors to use. Computers and Systems include the following:

Computers including:

TI99/4A
Timex Sinclair 1000
Sinclair ZX81
Commodore Amiga
Commodore Vic 20
Commodore 64
Commodore C64
Commodore Pet
Commodore Plus 4
Apple IIe
Apple Newton PDA
Atari 2600 (hundreds of games)
Atari 400
Kaypro (suitcase portable computer)
Panasonic Sr Partner (suitcase portable computer with builtin printer)
Tandy Radio Shack TRS-80 Model 1 Tandy
Color Computer 2 Tandy model
100 portable computer
Portable games including:

Merlin
Mattel Baseball
Coleco Quarterback
Mattel Football
Palm Pilot (original)
Coleco Pong
Milton Bradley Comp IV
8 inch floppy disks
Harvard Punch Cards
Hundreds of old computer magazines
Compute!
BYTE

Website: <http://vintagetechnologymuseum.org/>



ETHICS VILLAGE

Friday: 11:00 to 19:00,
Saturday: 11:00 to 18:00
Location: Modena -
Caesars Palace

Information security is ethically challenging. The field is based on the notion that in order to protect a system one must first be able to determine its vulnerabilities.

After the vulnerabilities have been identified, the difficulties multiply. Complications arise as we decide how to disclose that vulnerability, and how we apply solutions.

Unlike the professions of medicine and law, information security does not have a codified standard of ethics. Professionals in information security have yet to agree upon common ethical principles and many remain unconvinced of the possibility of establishing a universal framework that can address the realm of information security.

As a community, we need to explore the ethical situations arising from the information security domain. We are in need of innovative approaches to information security education that will equip information security professionals with more than just technical skills. We also need to cultivate dispositions that will incline those in the community to act ethically.

This involves cultivating a sensitivity to ethical issues and awareness of our own ethical blind spots in order to put our minds to work toward ethical analysis. To do this, we need to cultivate a wide range of knowledge, skills, and dispositions that will both enable and motivate us as a community to act ethically in the practice of our profession.

Village Schedule: <http://ethicsvillage.org/#sched>
Website: Twitter: @EthicsVillage
Twitter: WWW.EthicsVillage.org
Other: <http://ethicsvillage.org/#cfp>



LASER CUTTING VILLAGE

Location: Calibria - Caesars

Make your time for fir'n da laser at the laser cutting village, where you can cut, burn and engrave your tools!

This is the first ever trial of the laser cutting Village at Defcon 26!

Attendees can learn to cut and engrave a wide array of materials including wood, rock, glass, paper, leather, acrylic, Cork, cardboard, and other materials, using the intense power of light!

We will help users create projects, design art, customize items, and learn to use the various software associated with laser-cutters. The K40 laser, AKA "the cheap Ebay laser", is our primary entry point into the laser-cutting technology. We will share experience, and mods made to our K40 lasers, that make them perform better, produce higher quality cuts, and improve ease of use.

SKYTALKS

Location: Virginia City - Flamingo

Skytalks is a 'sub-conference' that gives a unique platform for researchers to share their research, for angry hackers to rant about the issues of their industry, and for curious souls to probe interesting issues, all without the watchful eye of the rest of the world.

With a strict, well-enforced "no recording" policy, research that is underway or critical of a vendor can be aired to your peers. You are talking to other people in the computer underground, and very few topics are taboo.

We invite the best of how DEF CON has been: the best of the computer underground -- in all its forms. Esoterica is as welcome as 0-day here.



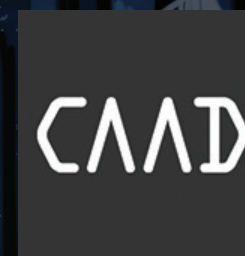
CANNABIS VILLAGE (PUFF PUFF HACK)

Friday: 10:00 to 17:00,
Saturday: 10:00 to 17:00
Location: Valley of
Fire - Flamingo

TLDR: Exploring DIY cannabis tech and examining the security posture of more established cannabis tech, products, services, and devices.

Cannabis has been a "hot ticket" tech and shows no signs of slowing. What happens when companies rush to first fill niches in the latest and greatest vertical? What do quickly hand-spun web-apps and an ever-forward compulsion towards the "internet-of-crap" get you? Gaping security flaws. Add it's precarious federal legal status in this shaky political climate and you've got a complicated yet intriguing technical landscape hackers should find familiar. Through Puff Puff Hack we aim to bring the hacker ethos from the DEF CON floor to the world of cannabis (and vice versa) by making & breaking point-of-sale or medical software & grow-op hardware, milling over the security & accountability of vendors, considering questions of legal protections & intellectual property, and by taking a deep look at the science, tech, and history of weed.

Village Schedule: http://www.bit.ly/puffpuffhack_sched
Website: www.puffpuffhack.com
Twitter: @puffpuffvillage
Other: Instagram: @puffpuffhack



CAAD VILLAGE

Friday: 10:00 to 17:30,
Saturday: 10:00 to 17:30
Location: Lake
Mead- Flamingo

CAAD Village focuses on AI security, especially on adversarial examples which can fool the neural network to be of

one class while being of other. So far, adversarial examples can be created for domains like image, audio, video, or text.

CAAD, a new section of GeekPwn Hacker Competition, would like to accelerate research on adversarial examples and improve AI security. At CAAD Village, there will be AI-hacking demos, presentations and the FIRST competition combines CTF and Adversarial Attacks & Defenses, called CAAD CTF.

Website: caad.geekpwn.org
Village Schedule: <http://blog.geekpwn.org>

VILLAGES

Website: caad.geekpwn.org
Twitter: @GeekPwn
Other: 2018.geekpwn.org

BLUE TEAM VILLAGE

Friday: 10:00-18:00,
Saturday: 10:00-16:00,
Sunday: 10:00-14:00
Location: Savoy - Flamingo

Blue Team Village at DEF CON (BTV) promotes defensive security knowledge and its

dissemination throughout the otherwise offensive security focus that is DEF CON. At the BTV, attendees will find valuable information on defensive security techniques, tools, research and concepts from industry leading experts, ranging in entry-level overviews through bleeding edge research. BTV focuses on the knowledge and experience needed in today's threat landscape, highlighting the hardening of environments, detection of intrusions, response to known incidents and addressing modern business requirements all geared to challenge the offensive security research addressed in the other DEF CON venues.

Through talks, the BTV presents industry experts will address best practices, advanced techniques, and strive to cover the massive arsenal of tools and research now available to defenders. Presentations will draw upon a breadth of experiences with diverse technologies.

Focusing on learning through hands-on experience and sharing one-on-one, break out events within the village provide both practical lab exercises with the latest tools and shared knowledge transfer of critical topics. In addition, a defensive-focused Capture the Flag (CTF) provides a contest format for both experienced and entry-level defenders to hone their skill set with a wealth of challenges.

Beyond the curated topics and events of the BTV, the space provides an informal gathering of like-minded individuals, providing a critically needed networking space for those whose professional responsibilities and/or personal passions align.

Website: <https://dcbtv.org>

contest that features Howdy Neighbor and the Industrial Control Systems (ICS) Range. This first of its kind CTF will be a slice of modern city life integrating both Internet of Things (IoT) and ICS environments with interactive components for competitors to test their skills and knowledge. The ICS Village delivers a compelling experience using real IT and industrial equipment for all skill levels and practitioner types.

The ICS Village will bring real components such as Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), Remote Telemetry Units (RTU), and actuators to simulate a realistic environment by using commonly components throughout different industrial sectors.

Website: <https://www.icsvillage.com>



CAR HACKING VILLAGE

Friday: 10:00 to 19:00,
Saturday: 10:00 to 18:00,
Sunday: 10:00 to 12:00
Location: Red rock- Flamingo

This year we will focus on autonomous vehicle technologies

such as lidar, adas, mapping, GPS, vision, V2V radio and other vehicle technology.

We would like to host 2 or 3 vehicle platforms.

Also we would like to have add a new area where we modify scooters like the one people drive around at trade shows in Vegas. This would be a competition style mini event in the village.

Village Schedule: <http://www.carhackingvillage.com/talks>
Website: www.CarHackingVillage.com
Twitter: @CarHackVillage

ICS VILLAGE

Location: Red Rock- Flamingo

The ICS Village equips industry and policymakers to better defend industrial equipment through experiential awareness, education, and training.

High profile Industrial Control Systems security issues have

grabbed headlines and sparked changes throughout the global supply chain. The ICS Village allows defenders of any experience level to understand the unique failure modes of these systems and how to better prepare and respond to the changing threat landscape.

Bring your laptop and win prizes! This year the ICS Village will be running Hack the Plan[e]t Capture the Flag (CTF)

SKYTALKS

FRI // AUG 10

09:00 **UNCLE G.** // BIGGEST IT SEC. FUCKUPS I'VE SEEN IN THE PAST 25 YEARS

10:00 **MASTERCHEN** // STALKER IN A HAYSACK

11:00 **SOLDIER OF FORTAN** // DECONSTRUCTING DEFENESTRATE.C: THE FIRST PUBLIC BUFFER OVERFLOW ON A MAINFRAME?

12:00 **MAGG** // WHEN INCIDENT RESPONSE MEETS REALITY

13:00 **WILLIAM KNOWLES & JAMES COOTE** // PRACTICAL ATTACK SIMULATIONS IN CNI: OH THE PERILS, OR OH THE FUN?

13:30 **RENDERMAN** // PENETRATION TESTING SEX TOYS: "I'VE SEEN THINGS YOU WOULDN'T BELIEVE"

14:00 **ETHAN GREGORY DODGE** // FROM MORMONLEAKS TO FAITHLEAKS

15:00 **LAURA H.** // OSINT IS FOR SOCCER MOMS

16:00 **BRITTANY "STRAITHE" POSTNIKOFF, SARA-JAYNE TERP** // ROBOTS AND AI: WHAT SCARES THE EXPERTS?

17:00 **DANIEL WILLIAMS (FBUS)** // THE LEAST COMMON DENOMINATOR STRATEGY (AKA "DON'T MAKE DEVOPS TOO EASY")

18:00 **WORNBT** // REAL SIMPLE BLUE TEAM SHIT

SAT // AUG 11

09:00 **DIMITRI** // WHAT HAPPENED BEHIND THE CLOSED DOORS AT MS

09:30 **SECURITY PANDA** // HTTP2 AND YOU

10:00 **3NCRIPT3D** // DON'T BRING ME DOWN: WEAPONIZING BOTNETS

11:00 **SIDRAGON** // THE ABYSS IS WAVING BACK...

12:00 **XAVIER ASHE** // CLOUD SECURITY MYTHS

13:00 **MIKE RAGGO & CHET HOSMER** // EXPLOITING IOT COMMUNICATIONS - A COVER WITHIN A COVER

14:00 **MARCELLE & KELLEY** // HACKING THE TECHNICAL INTERVIEW

15:00 **AMIT ELAZARI & KEREN ELAZARI** // LEVELING THE BUG BOUNTY PLAYFIELD INTRODUCING THE #LEGALBUGBOUNTY PROJECT

16:00 **SHAWN MERDINGER** // HEALTHCARE EXPOSURE ON PUBLIC INTERNET

17:00 **J3LENA** // THE CHALLENGE OF BUILDING AN SECURE AND SAFE DIGITAL ENVIRONMENT IN HEALTHCARE

18:00 **PHILIPPE DELTEIL** // MACABRE STORIES OF A HACKER IN THE PUBLIC HEALTH SECTOR (CHILE)

SUN // AUG 12

09:00 **BACE16** // MASTER BAITING! DON'T CLICK BAIT, CLICK YOURSELF

10:00 **STUMBLES THE DRUNK** // FACIAL RECOGNITION - LET ME LET YOU IN ON A SECRET

11:00 **MAGGIE MAYHEM** // SEX WORK AFTER SEXTA

12:00 **BRAIN & B9PLUS** // ALPHATHREAT SOUP: BURNING THREAT ACTORS WITH DATA

13:00 **NICK CANO** // "GAME RUNNER 2049: THE BATTLES FOUGHT BY THE KING OF THE REPLICANTS"

OFF THE RECORD.
NO VIDEO RECORDING ALLOWED.
BE THERE OR MISS IT FOREVER.

CHECK SKYTALKS INFO
FOR ANY SCHEDULE UPDATES

LOCATION INFO
FLAMINGO HOTEL,
VIRGINIA CITY ROOM

ART BY: CARBONCREATURES.COM
// FEATURING ADA



VILLAGES

THE MONERO BCOS VILLAGE

Contacts: michael@getmonero.org, ajit.hatti.sec@gmail.com
Location: Pompeian I



The Monero project is a privacy ecosystem which consists of the Monero core team, Monero research lab, Monero hardware team, Kovri, Openalias, and several other projects and work groups. The village presents technology serving privacy-conscious novice and advanced cryptocurrency users, inviting participation in a well-equipped and comfortable environment.

The Blockchain & Cryptocurrency Open Security Village (BCOS) is an effort to create a thriving community to make blockchain technology & cryptocurrencies more secure, robust and trustable. As they say at DEFCON, it takes a village to raise security level of any technology. The BCOS future is great, lets secure it.

Aside from our village keynotes, panels, workshops, and networking programs, you're invited to stop by to learn about parties, films, prize giveaways, and person-to-person guidance regarding blockchain and cryptocurrency technology.

A variety of hardware wallets, privacy merchandise, and the official village badge (a unique split-brained programmable MCU with powered moving lights and NFC interfaced EPROM storage) will be available for sale or display. Other educational materials are available as well.

FRIDAY, AUGUST 9TH

10:00-11:00: WELCOME SPEECH

We discuss various village announcements, an overview on our village and the events to come, an explanation of community ideology, and many educational materials.

11:00-12:00: KEYNOTE SPEECH - INSIDE MONERO

Howard Chu, CTO and Founder of Symas Corp. (@hyc_symas)
This talk will cover a brief introduction to cryptocurrency and blockchain. He will describe characteristics of Bitcoin, including its strengths and weaknesses. He will discuss how Monero approaches these similar challenges, and how it succeeds and struggles in different ways. He will explain how Monero works, why financial privacy is important, and what challenges Monero will face in the coming years.

12:00-12:30: CONTEST ANNOUNCEMENTS AND ROUND OF GIVEAWAYS!

Robin Renwick and Michael Schloh von Bennewitz
Join us as we explain educational resources and contests for attendees. Learn how to configure a wallet, run a node, mine, program a badge, connect to various services, learn about community events, and contribute. Hear about what prizes await those completing challenges, and to grease the wheels we start off with a round of giveaways to anybody visiting.

12:30-13:00: OPEN SOURCE HARDWARE AND THE MONERO PROJECT

Matthias Tarasiewicz, board member of the Open Source Hardware Association (@parasew)

Matthias will give an overview on Open Source Hardware, with a strong emphasis on (1) the AXIOM open source cinema camera (apertus) and (2) the Monero Open Hardware Wallet. Open Source Hardware (OSH) in difference to open source software has to face other challenges. He will outline the societal benefits of OSH and open source hardware as educational tools.

13:00-13:30: A RUNDOWN OF SECURITY ISSUES IN CRYPTOCURRENCY WALLET SOFTWARE

Marko Bencun, co-founder and software lead at Shift Devices

Software cryptocurrency wallets hold billions of dollars in value. We will run through as many security issues around this as we can in 30 minutes - from hilarious fails to subtle issues in the tech-stack.

13:30-14:00: WE DON'T NEED NO STINKIN BADGES

Michael Schloh von Bennewitz, organizer of the Monero Hardware Workgroup

The badge circuit designer speaks of hardware development, the village badge, and it's relationship to other Monero Hardware team projects. Michael will explain:

How to obtain a official BCOS Monero Village badge

What the badge is made of and what to do with it

He will spend nearly half the duration answering common questions from online interactions and questions from the audience. Sample badges will be passed around for inspection and demonstrated using a close range circuit camera.

14:00-16:00: HACK ON THE BITBOX HARDWARE WALLET

Stephanie Stroka and Marko Bencun, co-founder and software lead at Shift Devices

This is a hands-on session for developers new to firmware/embedded development. We will use the BitBox for hacking, which is a small portable USB-powered device featuring a screen and two touch sliders. This makes for a fun hacking environment. You will get a BitBox device and learn how write, compile, flash, and run firmware code to interact with the hardware, such as displaying something on the screen and taking user input via the sliders.

If time allows, we might venture into implementing a feature together, such as Bitcoin transaction verification and signing, or similar.

16:00-17:00: SCALING AND ECONOMIC IMPLICATIONS OF THE ADAPTIVE BLOCKSIZE IN MONERO

Francisco Cabañas, Monero Core Team member

The adaptive block size in Monero uses the CryptoNote excess size penalty. This excess size penalty leads to economic relationships between the block reward and the total fee revenue per block. It also presupposes that all the economic costs of transaction capacity expansion are proportional to the block size. We will discuss the implications of these economic relationships on proof of work (PoW) miner incentives and transaction fees as the

Monero block size scales. We will also discuss the extension of the CryptoNote excess size penalty to address transaction capacity expansion costs that do not scale linearly with the block size such as the verification time costs of bulletproofs.

The adaptive block penalty needs to scale with a variety of factors, including transaction size, verification time, bandwidth capacity, and hardware improvements.

17:00-18:00: HACKING A CRYPTO PAYMENT GATEWAY

Felix Honigwachs CEO GloBee, and Devin Pearson Project Architect GloBee

Devin and Felix lead a hands on mini workshop, demonstrating the utility and ease associated with integrating a cryptocurrency payment gateway in existing sales and marketing workflows. Illustrated on specialized machines, they lead novices to understand how to start accepting cryptocurrency payments in their networks.

SATURDAY, AUGUST 10TH

10:00-11:00: KEYNOTE SPEECH - EXCHANGE SECURITY

Philip Martin, VP of Security at Coinbase (@SecurityGuyPhil)

Philip explains BCOS contributions to blockchain, cryptocurrency, and how open security relates to seasoned business and core exchanges. Hear what BCOS can do for you as a blockchain user and cryptocurrency trader.

11:00-11:30: CONTEST SHOWCASE AND AWARD GIVEAWAYS!

Robin Renwick and Michael Schloh von Bennewitz

Learn what our colleagues developed in a day's contests and challenges, where prizes and giveaways are once again awarded to participants and the general public. Learn how to configure a wallet, run a node, mine, program a badge, connect to various services, learn about community events, and contribute.

11:30-12:00: MONERO'S EMERGING APPLICATIONS

Riccardo Spagni, Monero Core Team member and co-founder of Tari (@fluffypony)

Monero has several use-cases aligning with typical cryptocurrency and blockchain technologies; however, most don't know of the spinoffs and think tanks serving to push the boundaries of traditional cryptographic financial instrumentation. Riccardo will give his opinion on the direction of most recent Monero developments, striking comparisons with other privacy and currency applications, while giving concrete example of how Tari and GloBee are serving the Monero landscape of users, corporations, and payment processors.

12:00-14:00: WE PROGRAM OUR STINKIN BADGES!

Michael Schloh von Bennewitz, organizer of the Monero Hardware Workgroup

We will review the village badge and all its features in a read-only questions and answers (and complaints?) introduction. Then, we will discuss how a high-level review of controller chip process and workflow helped us gain knowledge on how to program our badges.

In the second hour, we form groups (according to programming cables and resources) to write and program "hello world" applications for our badges. We will learn to erase and debug the flash storage on the chip that controls lights on the badge.

Last, we consider how a homemade on-chip debugger is constructed and review relevant tools useful in programming MCUs and similar low-power circuits.

14:00-14:30: EXAMINING MONERO'S RING SIGNATURES

Justin Ehrenhofer, organizer of the Monero Community Workgroup (@JEhrenhofer)

Monero uses ring signatures to provide untraceability, but how effective are they? Justin will examine the potential use-cases and shortfalls of ring signatures. He will address the concerns of chain splits, public pool payouts, KYC/AML exchanges, and more. He will make recommendations on how to use Monero in a variety of use-cases, and how ring signatures can be improved to mitigate some of these threats.

14:30-15:00: SOME MINING-RELATED ATTACKS

Zhiniang Peng, security researcher at quihoo360 (check spelling!)

In this presentation, Zhiniang will present the several mining related attacks against various cryptocurrencies happened recently. For example, the fake mining attack against equihash mining pool and the coin-hopping attack against verge. He will demonstrate that there is huge attack surface in mining and propose several mitigations for it.

15:00-17:00: AN INTRODUCTION TO KOVRI

anonimal, organizer of the Kovri Project (@whoisanonimal)

Cryptocurrencies are based on an open peer-to-peer network. While this allows the network to be easily accessible, it leaves the potential network surveillance. Attackers could attempt to run a significant amount of this infrastructure and collect information about how transactions are relayed to associate transactions with others, censor transactions from being accepted by the network, and associating transactions with user IP addresses.

Kovri is a Monero Project that seeks to reduce the amount of meaningful network metadata that can be collected. It is an anonymizing router currently based on I2P's open specifications. Kovri will be incorporated into the most popular Monero wallets to protect the transaction broadcast and optionally hide all knowledge that the user is running a Monero node.

Kovri will ship with a common API that can be used by several other projects, including other cryptocurrency projects. Kovri will benefit its users by providing more anonymity, and it will benefit the I2P network by providing more entropy and infrastructure.

This talk is a practical introduction on how to use and understand Kovri.

17:00-18:00: PRIVACY AND SECURITY PANEL

Justin Ehrenhofer, moderator (@JEhrenhofer)

This panel will feature the following people:

Shamiq I, application security manager at Coinbase

VILLAGES

Paul Shapiro, CEO of MyMonero (@tweetingpauls)
anonimal, organizer of the Kovri Project (@whoisanonimal)
Riccardo Spagni, Monero Core Team member
and co-founder of Tari (@fluffypony)

We will discuss important and trending cryptocurrency-related topics with plenty of time to answer your audience questions.

18:00-18:30: PARTY ANNOUNCEMENT!

Cinnamonflower and pwreycle

SUNDAY, AUGUST 11TH

10:00-10:45: THE GOOD, THE BAD, AND THE PRIVATE: BUILDING AND BREAKING SAFE CRYPTOCURRENCIES

Sarang Noether, Monero Research Lab contributor

Privacy is poorly defined, and this is often true of cryptographic assets. Despite what much early coverage suggested, the use of a blockchain as ledger for digital assets inherently provides significantly less privacy than may be desired. Fortunately, clever uses of algebra and number theory have led to cryptocurrency projects with far better guarantees toward privacy, security, and fungibility. In this talk, we'll look at the various ways that mathematical techniques are applied to build safe cryptocurrencies, and examine some of the weaknesses and attacks seen throughout several projects' histories

10:45-11:00: CONTEST SHOWCASE, AWARDS, AND GIVEAWAYS

Robin Renwick and Michael Schloh von Bennewitz

Robin and Michael make one last try at delivering free merchandise into the hands of challenge takers as well as the general public!

11:00-11:30: MONERO'S DIFFERENTIATED COMMUNITY

Justin Ehrenhofer, organizer of the Monero Community Workgroup (@JEhrenhofer)

Monero's community is different from all other cryptocurrency communities. It seeks to straddle the divide between decentralization and effective management. Justin will discuss how the community consists of various self-organizing workgroups that communicate with the wider community to solicit support. He will discuss the Community Workgroup's role in providing resources and creating important connections. He will discuss how Monero raises funds for projects and supports its top contributors. Finally, he will examine certain community behaviors as evidenced through specific events.

11:30-12:00: PRIVACY AND BLOCKCHAIN: A BOUNDARY OBJECT PERSPECTIVE

Robin Renwick, blockchain privacy researcher at University College Cork/State Street Advanced Technology Centre
Blockchain technology emerged at the beginning of 21st century, becoming renowned for its role in enabling cryptocurrencies such as Bitcoin. While the majority view blockchain as revolutionary, their perspective of such revolution differs. These differences become especially meaningful for two reasons. First, each of these groups

is actively contributing to the development of blockchain either directly (as is the case for academic researchers, and protocol developers), or indirectly (as is the case for investors and regulators). Thus, each is inevitably trying to direct and influence the evolution and growth of the technology as they see fit. Second, a central feature of blockchain technologies is that it is a 'distributed ledger', i.e. a public record of interactions visible to all nodes on the network. This has the potential to create a single, complete historic reservoir of data, the anonymity, fungibility, and transparency of which has significant social and economic implications for individual liberty and/or legal accountability, depending on one's perspective. The objective of this talk is to outline how different attitudes to privacy are likely to impact the development of blockchain technologies, and especially Monero. These attitudes will be drawn from qualitative analysis of semi-structured interviews carried out with practitioners from five key social worlds, namely corporate architects, regulators, users/investors, cryptographic researchers, and protocol developers.

12:00-12:30: STEALING CRYPTOCURRENCY. 2 FACTOR ISN'T A FACTOR

Rod Soto, security researcher with Hackmiami (@rodsoto); and Jason Malley compliance and IT security (@n00bznet)

This presentation will show how malicious actors are actively taking advantage of the use of SMS as second authentication factor to prove identity. These vulnerabilities enable malicious actors to obtain SMS messages, then proceed to reset and take over all users accounts starting with email accounts with access to financial, social media, and corporate accounts. SMS should be discarded as a second form of authentication. This presentation will also provide alternative authentication methods to compensate SMS deprecation.

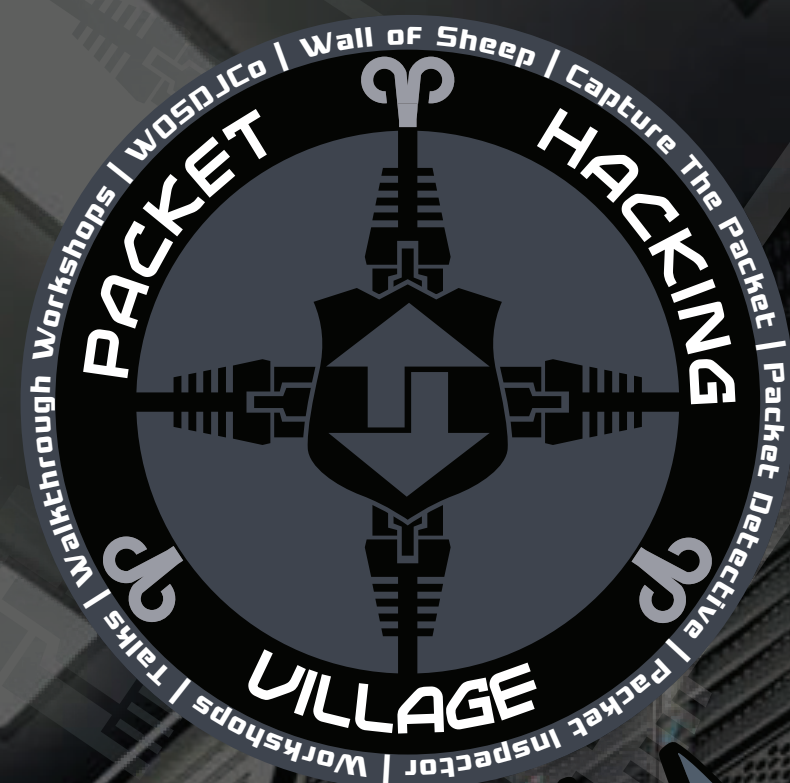
12:30-13:00: MONERO PROJECT'S VULNERABILITY RESPONSE PROCESS

anonimal, organizer of the Kovri Project (@whoisanonimal)

This presentation will explain the Monero Project's approach to vulnerability response. We will cover the project's vulnerability response process and use of HackerOne.

13:00-14:00: VILLAGE SUMMARY, CLOSING, THANKS, AND LIGHTS OUT

Diego "rehrrar" Salazar and his exhausted village staff
With his floor staff singing backup, Diego takes us on a trip down memory lane. His closing speech includes snippets of recent Monero developments in the community as well as the preceding few days at DefCon 26, thanking the public and organizers for supporting our first village ever.



Friday 10:00 a.m. (opening ceremony at 10:10 a.m.)

Saturday 9:00 a.m.

Sunday 10:00 a.m. (closing ceremony at 2:10 p.m.)

Location: On the third floor Neopolitan area in Ceasars.

The Packet Hacking Village is where you'll find network shenanigans and a whole lot more. There's exciting events, live music, competitions with awesome prizes, and tons of giveaways. PHV welcomes all DEF CON attendees and there is something for every level of security enthusiast from beginners to those seeking a black badge. This village was created to help enlighten attendees through education and awareness while focusing on defense and blue team techniques.

Wall of Sheep gives attendees a friendly reminder to practice safe computing through strong end-to-end encryption. PHV Speakers, Workshops, and Walkthrough Workshops delivers high quality content for all skill levels. Packet Detective and Packet Inspector offers hands-on exercises to help anyone develop or improve their Packet-Fu. WoSDiCo has some of the hottest DJs at con spinning live for your enjoyment. Finally... Capture the Packet, the ultimate cyber defense competition that has been honored by DEF CON as a black badge event for seven of the eight years of it's run.

Read on to see all of our events!



/wallofsheep



@wallofsheep





Capture The Packet - CTP

The time for those of hardened mettle is drawing near; are you prepared to battle? Compete in the world's most challenging cyber defense competition based on the Aries Security Cyber Range. In order to triumph over your competitors, contestants must be well rounded, like the samurai. 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.

The Dark Tangent has asked that we extend your time in the labyrinth and this has caused the difficulty of challenges to be amplified, 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.

Teams consist of up to 2 players and can register at the CTP table in the Packet Hacking Village.



WALL OF SHEEP

Wall Of Sheep

An interactive look at what could happen if you let your guard down when connecting to any public network, Wall of Sheep passively monitors the DEF CON network looking for traffic utilizing insecure protocols. Drop by, hang out, and see for yourself just how easy it can be! Most importantly, we strive to educate the "sheep" we catch, and anyone else interested in protecting themselves in the future. We will be hosting several 'Network Sniffing 101' training sessions using Wireshark, Ettercap, dsniff, and other traffic analyzers.



Wall of Sheep DJ Community - WoSDJCo

Come chill with us while we play all your favorite Deep, underground house, techno, breaks, and DnB beats mixed live all weekend by your fellow hacker DJs. We will provide the soundtrack for all your epic PHV hax, just like we do every year.

PACKET DETECTIVE

ARIES SECURITY

Packet Detective

Looking to upgrade your skills or see how you would fare in Capture The Packet? Come check out what Packet Detective has to offer! A step up in difficulty from Packet Investigator, Packet Detective will put your network hunting abilities to the test with real-world scenarios at the intermediate level. Take the next step in your journey towards network mastery in a friendly environment still focused on learning and take another step closer to preparing yourself for the competitive environment of Capture The Packet.

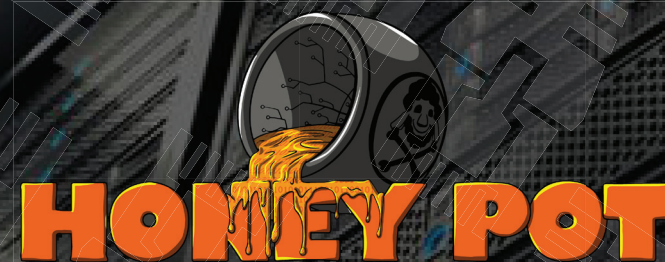
PACKET INSPECTOR

ARIES SECURITY

Packet Inspector

Taking the place of Packet Detective as your introduction to network analysis, sniffing, and forensics. Do you want to understand the techniques people use to tap into a network, steal passwords and listen to conversations? Packet Inspector is the place to develop these skills! For well over a decade, the Wall of Sheep has shown people how important it is to use end-to-end encryption to keep sensitive information like passwords private. Using a license of the world famous Capture The Packet engine from Aries Security, we have created a unique way to teach hands-on skills in a controlled real-time environment.

Join us in the Packet Hacking Village to start your quest towards getting a black belt in Packet-Fu.



Walkthrough Workshops - Learn to build Honey Pot's

The Packet Hacking Village brings yet another Def Con premiere: Walkthrough Workshops, where you will go on a self-guided journey to building your own honey pot, taking it live and hopefully trapping some unsuspecting users. Fear not though, like with all our other training events, we will have helpful and knowledgeable staff on hand to assist you along the way!



PHV Talks

Back for a sixth year, we continue to accept presentations focusing on practice and process while emphasizing defense. Speakers will present talks and training on research, tools, techniques, and design, with a goal of providing skills that can be immediately applied during and after the conference. Our audience ranges from those who are new to security, to the most seasoned practitioners in the security industry. Expect talks on a wide variety of topics for all skill levels.

Updated schedule available at: <https://wallofsheep.com/pages/dc26>



PHV Workshops

A returning favorite from last year, we have hands-on labs and training sessions from an amazing line-up of instructors covering beginner to advanced level material. See our website for updated schedules.



Schedule and speaker bios available at: <https://wallofsheep.com/pages/dc26>

Friday, August 10th

10:00 - 11:00

Mallet: A Proxy for Arbitrary Traffic

Rogan Dawes, Senior Researcher at SensePost

Mallet is an intercepting proxy for arbitrary protocols. More accurately, it is a framework for building proxies for arbitrary protocols. Mallet provides the basics required of all proxies: A way to receive the data, a way to send the data, and a user interface to intercept and edit the data. It builds on the Netty project, and as such has access to a large, well-tested suite of protocol implementations that can be used to transform a stream of bytes into useful, high-level protocol objects. This workshop will introduce attendees to Mallet, and show how to construct pipelines of arbitrary complexity, to successfully decode and intercept messages in various protocols, as well as automating modifications of the various messages. A basic familiarity with Java will enhance the delegate's understanding of what they are taught, but is not a requirement.

11:00 - 12:00

Rethinking Role-Based Security Education

Kat Sweet, Duo Security

How do we scale a deeper level of security awareness training without sacrificing efficacy? This talk will explore strategies and tactics for developing security education based on employees' roles, access, and attack surface while designing not only for efficiency but also for effectiveness.

12:00 - 13:00

PacketWhisper: Stealthily Exfiltrating Data and Defeating Attribution Using DNS and Text-Based Steganography

TryCatchHCF

Data exfiltration through DNS typically relies on the use of DNS query fields to exfiltrate data via the attacker's DNS server. This approach has several shortcomings. The first is attribution, since attackers end up creating a trail back to their own infrastructure. The second is awareness, as DFIR analysts have made careful study of DNS fields as exfiltration vectors. The third is access, since companies are increasingly using DNS server whitelisting to prevent or alert on outgoing DNS queries to servers controlled by attackers. The presentation will include a demonstration of PacketWhisper, a new tool written in Python, that automates all of these steps for you. PacketWhisper will be made available on GitHub to coincide with this session (<https://github.com/TryCatchHCF>).

13:00 - 14:00

Target-Based Security Model

Garett Montgomery, Principal Security Research Engineer at BreakingPoint (Ixia/KeySight)

The Target-Based Security Model is essentially a framework that breaks down attacks to their component

level. This breakdown makes it easy to see what the 'best' security controls are - as well as alternative security controls that could also be applied. Its not so much something new, as it is a new way for the industry to communicate about security. In much the same way that the OSI model allows for developers to know they are talking about the same thing, a common security model allows security professionals to communicate in a vendor agnostic manner. Think of it as a translation tool for vendor speak.

14:00 - 15:00

Protecting Crypto Exchanges from a New Wave of Man-in-the-Browser Attacks

Pedro Fortuna, CTO and Co-Founder of Jscrambler

In this talk, we will detail how Man-in-the-Browser (MITB) attacks work, from account take over to moving out the coins to attacker-controlled wallets. We'll discuss current defenses e.g. multi-factor authentication or strong SSL encryption and why they are failing to mitigate this type of attacks.

15:00 - 16:00

Freedom of Information - Hacking the Human Black Box

Elliott Brink, Senior Penetration Tester at RSM US LLP

FOIA (otherwise known as the Freedom of Information Act or FOI/Freedom of Information in Australia) are government-based initiatives to permit the public to request information on various government records. In practice, these acts enable transparency of the operations of government to the masses with relative ease. In reality, submitting FOI requests can be a cumbersome and frustrating process for citizens. Attendees will gain practical knowledge about: what FOIA is, the caveats of FOIA, how you can utilize FOIA on red team engagements and other open source intelligence gathering activities and finally the results of my research in multiple requests to intelligence agencies.

16:00 - 17:00

Car Infotainment Hacking Methodology and Attack

Surface Scenarios

Jay Turla, Application Security Engineer at Bugcrowd

In this talk, join Jay as he presents his own Car Hacker's Methodology in finding security bugs in order to pwn a car's infotainment system without having to do a drive by wire or CANbus hacking tools but will simply point out the common attack surfaces e.g WiFi, Bluetooth, USB Ports, etc. and some scenarios on how to exploit it just like how he popped a shell or issue an arbitrary command in his car which he tweeted in Twitter before.

17:00 - 18:00

Swiss Cheese Holes in the Foundation of Modern

Security - CERT VU#919801

Chris Hanlon, Founder of SecurityAlliance.ca

In this talk we briefly introduce common SMTP/TLS implementation weaknesses explain how governments, criminals, and malicious insiders can exploit them to remotely reset account passwords, create/update/delete firewall rules, control windows desktops/laptops, access online backup systems, download full-disk Encryption Keys, watch security cameras, listen to security camera microphones, control social media accounts, and takeover AWS virtual machines.

18:00 - 19:00

Mapping Wi-Fi Networks and Triggering on Interesting Traffic Patterns

Caleb Madrigal, Applied Researcher at Mandiant/

FireEye

In this talk, we'll use this tool to explore some of the surprisingly-informative data floating around in the radio space, and you'll come away with a new skill point or two in your radio hacking skill tree, as well as a new magical weapon... I mean tool.

Saturday, August 11th

10:00 - 10:30

Ducky-in-the-Middle: Injecting Keystrokes into Plaintext Protocols

Esteban Rodriguez, Security Consultant at Coalfire Labs

This talk will cover the basics of protocol analysis using Wireshark and lead into analyzing two custom application protocols used for extending the mouse and keyboard of a remote system. The two applications covered are HippoRemote, and iOS app to use a iPhone as a trackpad and keyboard, and Synergy, an application to allow for control of multiple operating systems with one mouse and keyboard. By performing a MITM attack, an attacker can abuse this protocols to send keystrokes to a remote machine to gain remote code execution similar to a USB rubber ducky attack. The talk will also discuss mitigations and open source code will be provided for exploitation. The target audience should have a basic understanding of Wireshark, ARP spoofing, and reverse shells.

10:30 - 11:00

How to Tune Automation to Avoid False Positives

Gita Ziabari, Senior Consultant Engineer at Verizon

This talk will cover techniques to design a reliable automated tool in security. We will discuss about techniques of tuning the automation to avoid false positives and the many struggles we have had in creating appropriate whitelists. We will walk through steps of creating an automated tool and the essential factors to be considered to avoid any false positive.

11:00 - 11:30

wpa-sec: The Largest Online WPA Handshake Database

Alex Stanev, CTO of Information Services at JSC

During the talk I will explain how wpa-sec (a world wide WPA handshake capture project) works, provide statistics and a lot of internals on optimization and how to use the database as OSINT source during pentests and red team actions.

11:30 - 12:00

Capturing in Hard to Reach Places

Silas Cutler, Senior Security Researcher at CrowdStrike

It's easy for us to take for granted when tools allow us to start capturing network traffic without any real hardships. However, what happens when the data you want isn't so easy to capture. This talk will look at two cases in which environments needed to be bent in order to capture the data needed for analysis.

12:00 - 12:30

An OSINT Approach to Third Party Cloud Service Provider Evaluation

Lokesh Pidawekar, Senior Cloud and Application Security Engineer at Cisco

In this talk, the attendees will learn about various methods of identifying security posture of the third-party cloud service using information available on Internet, how to use this information for performing cloud service review and improve their own cloud offerings. This can also supplement the tedious questionnaire process and provide an option to fast track the vendor reviews.

12:30 - 13:00

Bitsquatting: Passive DNS Hijacking

Ed Miles, Security Researcher at DiDi Labs

The Domain Name System is one of the foundational technologies that allow the internet to function, but unfortunately, DNS is surprisingly brittle to certain issues, such as bitsquatting. Lookups to names that are a "bitflip" away from well-known sites (like 'amczon.com' instead of 'amazon.com' since 'c' and 'a' have a single bit difference) can be caused by memory failing due to defect or overheating situations, rogue cosmic rays, or even (allegedly) radiation caused by nuclear reactions. In the end, attendees should leave with knowledge of the prevalence of bitsquatting and how it has evolved since the phrase was coined 8 years ago, as well as a few techniques for analyzing bitsquatting data and drawing some interesting conclusions.

13:00 - 13:30

Turning Deception Outside-In: Tricking Attackers with OSINT

Hadar Yudovich, Tom Sela, Tom Kahana, Security Researchers at Illusive Networks

In this talk, we will present research we conducted to answer these questions, and introduce a tool you can use to "try it at home." We first took a deeper look at various OSINT resources-social media, paste sites, public code repositories, etc.-to refine our picture of the types of publicly-available data, attackers might use to further an attack. Then we planted various deceptive information. For example, on PasteBin we created a fake "paste" page containing a dump of fake credentials. On GitHub we created a fake repository

of code containing “accidental” commits (git commit -am ‘removed password’). Next, we paired these deceptions with relevant data and user objects within a simulated network environment. We then started monitoring and waited for an attacker to bite.

13:30 - 14:00

Defense in Depth: The Path to SGX at Akamai

Sam Erb, Software Engineer at Akamai Technologies

In this presentation you will learn how Akamai has spent the past 4 years working toward preventing the next TLS heartbleed incident. Nothing hypothetical, only deployed defense-in-depth systems will be discussed. This talk will include how we deployed Intel SGX at scale in our network.

14:00 - 14:30

Building A Teaching SOC

Andrew Johnson, Information Security Officer at Carnegie Mellon University

Effective security monitoring is an ongoing process. How do you get everyone participating? How do you on-board junior colleagues to continuous improvement? The purpose of this presentation is to show methods for encouraging participation from all members of the security monitoring team as well as tactics for communicating effective with the organization.

14:30 - 15:00

Normalizing Empire’s Traffic to Evade Anomaly-based IDS

Utku Sen, Senior R&D Engineer at Tear Security
Gozde Sinturk, R&D Engineer at Tear Security

In this talk, we will discuss one of the most famous post-exploitation tool, Empire, against a payload-based anomaly detection systems. We will explain how to normalize Empire’s traffic with polymorphic blending attack (PBA) method. We will also cover our tool, “firstorder” which is designed to evade anomaly-based detection systems. The firstorder tool takes a traffic capture file of the network, tries to identify normal profile and configures Empire’s listener in such way.

15:00 - 16:00

Grand Theft Auto: Digital Key Hacking

Huajiang “Kevin2600” Chen, Security Research at Ingeek

Jin Yang, Independent Security Researcher

In this talk, we will reveal the research and attacks for one of digital car keys system in the current market. By investigating how these features work, and how to exploit it through different possibles of attack vectors, we will demonstrate the security limitations of such system. By the end of this talk, the attendees will not only understand how to exploit these systems also which tools can be used to achieve our goals.

16:00 - 17:00

Ridealong Adventures: Critical Issues with Police Body Cameras

Josh Mitchell, Principal cybersecurity Consultant at Nuix

At this talk, we will be introducing tactics, techniques, and procedures to assess the security of these devices. We will cover attacks against the physical devices, RF components, smartphone app’s, and desktop software.

The capabilities demonstrated and discussed will encompass publicly and privately available technologies. Additionally, the talk will cover multiple products and vendors, shedding light on industry wide issues and trends. Finally, we will be releasing software to detect and track various devices and tie these issues into real world events.

17:00 - 18:00

IoT Data Exfiltration

Mike Raggo, CSO of 802 Secure, Inc.

Chet Hosmer, Owner of Python Forensics

In this session we explore this new frontier by focusing on new methods of IoT protocol exploitation by revealing research conducted over the last 2 years. Detailed examples will be provided, as well as demo of a python tool for exploiting unused portions of protocol fields. From our research, we’ll also reveal new methods of detecting aberrant behavior emanating to/from these devices gathered from our lab and real world testing.

Sunday, August 12th

11:00 - 12:00

Microcontrollers and Single Board Computers for Hacking, Fun, and Profit
gh057

With the skyrocketing popularity of microcontrollers and single board computers, the cost barrier to entry for security applications has been reduced significantly and has created a host of new possibilities. gh057 will demonstrate three devices he built to solve specific problems: an ATTiny85 “Poor Man’s Rubber Duck”, an ESP8266 wrist-mounted network scanner and a Raspberry Pi multi-user mobile network analyzer.

12:00 - 13:00

Fishing for Phishers. The Enterprise Strikes Back!

Joseph Muniz, Cisco

Aamir Lakhani, Fortinet

This talk will cover how to build an artificial environment and develop anti phishing tools used to respond to phishing attempts. Results could include owning the attacker’s box “hypothetically” since some legal boundaries could be crossed.

13:00 - 14:00

What Do You Want to be When You Grow Up?

Damon “ch3f” Small, Technical Director at NCC Group North America

The speaker will describe his experiences as a 22-year veteran of IT and infosec, both from the perspective of working for internal support teams and as a client-facing consultant. In addition to direct observations, this presentation will include the perspectives of other infosec pros that currently work in various capacities in our industry. The goal is not to answer the question of how to successfully develop one’s career, as such, but rather to continue the dialogue of what is important to us as we develop our future experts and leaders.



Schedule and speaker bios available at:
<https://wallofsheep.com/pages/dc26>

Friday, August 10th

11:00 - 12:30

Reverse Engineering Malware 101 by Malware Unicorn

This workshop provides the fundamentals of reversing engineering (RE) Windows malware using a hands-on experience with RE tools and techniques. Attendees will be introduced to RE terms and processes, followed by basic x86 assembly, and reviewing RE tools and malware techniques. It will conclude by attendees performing a hands-on malware analysis that consists of Triage, Static, and Dynamic analysis.

13:00 - 15:00

Advanced APT Hunting with Splunk by Ryan Kovar and John Stoner

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. Then we look deep in the data using Splunk and OSINT to find the APT activity riddling a small startup’s network. We walk you through detecting lateral movement, the P of APT, and even PowerShell Empire. Then at the end, we give you a similar dataset and tools to take home and try newly learned techniques yourself.

15:30 - 17:00

Finding and Attacking Undocumented APIs with Python by Ryan Mitchell

Write Python web bots using Selenium and BrowserMob Proxy to crawl the Internet looking for non-public APIs. We will look at several ways to identify vulnerabilities in discovered APIs as a means for penetration testing and large scale data gathering. Participants should have some Python experience, as well as a familiarity with HTTP requests.

17:30 - 19:00

Serious Intro to Python for Admins by Davin Potts

Intended for an audience of IT managers and admins who are either responsible for systems with deployed Python apps and/or interested in the security implications of developing their own tools/scripts/apps in Python. This will be a hands-on exercise from start to finish designed to leave you with a sense of the mentality of Python and an ability to quickly look up what you need when expanding your knowledge of Python in the future. Prior programming experience not required. However it would be helpful if you’ve seen lots of Monty Python skits before.

Saturday, August 11th

09:30 - 13:30

Kali Dojo Workshop

by Johnny Long

Kali Linux can be deeply and uniquely customized to specific

needs and tasks. In this workshop, we will customize Kali Linux into a very specific offensive tool, and walk you through the process of customization step by step. We will create a custom Kali ISO that will: load very specific toolsets; define a custom desktop environment and wallpaper; leverage customized features and functions; launch custom tools and scripts; install Kali automatically, without user intervention as a custom “OS backdoor”. This workshop will guide you through all the aspects of Kali customization and give you the skills to create your own highly-customized Kali ISO, like the much feared Kali “ISO of Doom”.

14:00 - 16:00

Intense Introduction to Modern Web Application Hacking

by Omar Santos and Ron Taylor

This course starts with an introduction to modern web applications and immediately starts diving directly into the mapping and discovery phase of testing. In this course, you will learn new methodologies used and adopted by many penetration testers and ethical hackers. This is a hands-on training where will use various open source tools and learn how to exploit SQL injection, command injection, cross-site scripting (XSS), XML External Entity (XXE), and cross-site request forgery (CSRF). We will wrap up our two hour fast-paced course by unleashing students on a vulnerable web application with their newly found skills.

16:30 - 18:00

Mallet, An Intercepting Proxy for Arbitrary Protocols

by Rogan Dawes

Mallet is an intercepting proxy for arbitrary protocols. More accurately, it is a framework for building proxies for arbitrary protocols. Mallet provides the basics required of all proxies: A way to receive the data, a way to send the data, and a user interface to intercept and edit the data. It builds on the Netty project, and as such has access to a large, well-tested suite of protocol implementations that can be used to transform a stream of bytes into useful, high-level protocol objects. This workshop will introduce attendees to Mallet, and show how to construct pipelines of arbitrary complexity, to successfully decode and intercept messages in various protocols, as well as automating modifications of the various messages. A basic familiarity with Java will enhance the delegate’s understanding of what they are taught, but is not a requirement.

Sunday, August 12th

11:00 - 13:00

Advanced APT Hunting with Splunk by Ryan Kovar and John Stoner

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. Then we look deep in the data using Splunk and OSINT to find the APT activity riddling a small startup’s network. We walk you through detecting lateral movement, the P of APT, and even PowerShell Empire. Then at the end, we give you a similar dataset and tools to take home and try newly learned techniques yourself.

CONTESTS

AI VILLAGE JEOPARDY

In a jeopardy style CTF, contestants (if we are provided the full space requested) will be able to compete and learn by working through our challenges categorized in groups such as "classification", "clustering", and "attacking machine learning models". Participants will be provided a docker image will all datasets, questions (in IPython notebooks), and submission APIs needed to compete. Educational materials will be provided for initial (novice level) challenges to ensure that all contestants have a baseline understanding of the core concepts needed to compete.

Location: AI Village

Twitter: @aivillage_dc

Website: <http://jeopardy-ctf.aivillage.org>

BADGELIFE CONTEST

Badges have been around DEF CON for years, and badge hacking happens every year! This year, let's make it an official contest! Let's award prizes! Let's judge badges on originality, functionality, best counterfeit, and our personal favorite OMGWTFBBQ!

Location: Hardware Hacking Village

Twitter: @dcbadgelife

Website: <http://badgelife.org>

CMD+CTRL



CMD+CTRL is bringing two new vulnerable websites that participants will be competing to find vulnerabilities in.

Vulnerabilities are automatically detected and award points when they're exploited. There are over 100 different vulnerabilities, including SQLi, XSS, password cracking, and more. Come put your red team skills to the test and compete to find the most web vulnerabilities!

There will be easy challenges and reference material for beginners, as well as a hardened application to challenge experienced hackers.

Location: Contest Area

Hours: Friday 1000-1800, Saturday 1000-1800

Twitter: @cmdnctrl_defcon

COINDROIDS



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, or assemble your hacker-fam and compete in the quest to infiltrate Imperial One.

New to cryptocurrencies? No DEFCOIN to play with? Not a problem! Just come visit our booth in the contest area and we can help get you started.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @coindroids

Website: <https://www.facebook.com/Coindroid/>

CRACKMEIFYOUCAN

As a part of authorized penetration tests of companies' internal corporate networks and external websites, you have captured a large number of password hashes and some encrypted files of various types. You owned the firmware of some weird devices, and got hashes. You found corrupted backups with partial password hashes in them. You found password-protected ZIP and RAR files and you want to know what's inside. You were able to do a SQL injection, and extract the users' hashes from the database. But now, you have to crack all these hashes. In it's 7th year, Crack Me If You Can (CMIYC) is the premiere password cracking contest. We challenge teams of the world's best password crackers. And force them to share their knowledge, tips, and tricks with the community. The challenges presented in the 2010 contest are now trivial and easily completed by even a novice password cracker. So, in 2018, we hope to introduce new challenges that will continue to push the boundaries of what is possible with password recovery.

The contest is geared in a way so that even beginner password crackers will get some points, and hopefully learn along the way. Fire up your GTX 2080s and EC2 clusters. Ask your boss for time on that super computer your company has. Buy a CRAY on ebay. Email your college professor and ask for your account to be re-enabled on the cluster. Get a few extra box fans. You are going to need it all. Stop wasting your GPUs on playing Minecraft, there are passwords to crack!

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @crackmeifyoucan

Website: <https://contest.korelogic.com/>

DEF CON 26 CREATIVE WRITING SHORT STORY CONTEST

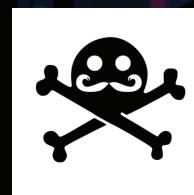
The DEF CON Short Story contest is a pre-con contest that is run entirely online utilizing the DEF CON forums. This contest follows the theme of DEF CON for the year and encourages hackers to roll up their sleeves and write the best creative story that they can. The Short Story Contest encourages skills 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.

Location: The Internets

Hours: All

Twitter: @dcshortstory

DEF CON BEARD AND MOUSTACHE CONTEST



Held every year since DEF CON 19 in 2011 (R.I.P. Riviera), the DEF CON Beard and Moustache Contest highlights the intersection of facial hair and hacker culture.

Location: Contest Area Stage

Hours: Friday 1800-2000

Twitter: @DCBeardContest

Website: <http://www.dcb beard.com/>

DEF CON BLITZ CHESS TOURNAMENT

The first-ever DEF CON Chess Tournament, in Blitzkrieg format, in which there will be just 5 minutes on each player's clock. During the tournament, each player will play every other player one time. A victory is 1 point, a draw 1/2, and a loss 0. At the end of the tournament, the player with the highest score wins the grand prize and a trophy. In the event of a tie, there will be a sudden death playoff between the highest scorers to determine the champion.

Location: Contest Area Stage

Hours: Saturday 1800-2000

DEF CON HAM RADIO FOX HUNTING CONTEST

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 DEF CON 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 to a larger puzzle, requiring participants to piece together the information broadcasted from each transmitter. Once they've decoded the final puzzle, they will be sent to find one final ultra low power transmitter broadcasting a passphrase which they will enter on a contest website and receive their trophy for completing the contest. 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 DEF CON to help people who find themselves stuck.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Website: <http://defcon26foxhunt.com>

DEF CON DARKNET



The DarkNet project is an online and in person game in which players interact with an chat bot that sends them on quests which teach as well as challenge them. Technical challenges related to

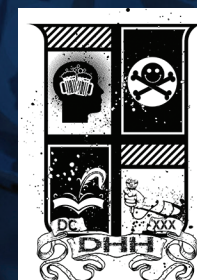
hacking and security are the most prominent. Each quest line requires the players to work independently or together to solve puzzles, research ciphers, learn new technologies such as PGP or Tor in order to gain points and progress. Many, but not all, of our quests have an in-person component -- we have in the past had a lock picking challenge box at our table, an RFID reader challenge, and badge kits that are involved in making progress in certain parts of the game. We collaborate with other Events, Villages and Contests to share content and send people around DEF CON to learn new things -- almost like a mini-DC101 program with a game around it.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Website: <https://dcdark.net>

DRUNK HACKER HISTORY



One night only at DEF CON 26, Drunk Hacker History is back by popular demand for a 4th historic year! The past three years proved to the entire galaxy that in the game of intoxicated nostalgic recall, there are no losers and those who won, lost. The DEF CON community has a history of sorts. It is a history filled with mephitic adventures, quarter-truths, poor life choices, incontinence, and various forms of C2H6O. This year, we will connect our

stacks to extract some of the most celebrated, exaggerated and entertaining moments in Hacker History through the interpretation of a group of well-trained participants. In the end, we will, again, crown the Drunkest Hacker in History and you, the audience, will rejoice! Hosted by c7five & jaku, if you like eating from an 80s candy cannon, "Cats" the musical, and feats of strength, you won't want to miss the return of Drunk Hacker History! Presented in DEF CON 4D and made possible by a grant from monkeyhelpers.org.

Location:

Hours: Saturday Night -

Twitter: @drunkHackerHist

DEF CON SCAVENGER HUNT



Do you have specialty skills that you haven't found an outlet for? Like making replicas of colonial era Presidents heads out of

macaroni and cheese or stitching wool sweaters for Venus fly traps? Well as it turns out there's a competition made special just for you! Come on down to the DEF CON Scavenger Hunt, now in its 21st year! We are the contest that you might not have known by name but you've probably seen, heard, or smelled all over DEF CON. With competitions that involve you with almost every aspect of DEF CON; we're arguably the best way you can spend your weekend. First through third place will receive fabulous prizes, while all other participants will presumably walk away with a little more dignity left.

CONTESTS

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @DefConScavHunt

Website: <http://defconscavhunt.com>

D(STRUCTION)20 CTF

Part CTF, part lemon race, part game show, part demolition derby, the D(struction)20 CTF is a contest best played with a low-cost, usable, rugged, and powerful hacking platform! Bring your "indestructible" phones, your single-board computers with welded cases, or just take that old clunker gathering dust in the closet and put it to good (and possibly hilarious) use! Periodically during the competition, a random contestant from the leaderboard will roll the d20 of Destruction to decide what will happen to their rig. If they're very lucky, they roll a natural 20 and no damage will be inflicted! Otherwise, the d20 of Destruction will decide what type of damage will be done to their rig, be it physical impact, intense vibration, or something else! If the rig survives their chosen fate, the contestant may continue playing, but either way, rolling the d20 of Destruction results in a big point bonus that may make the difference between winning and losing, even if the rig is destroyed in the process!

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000 Contest Area Stage - Saturday 1200-1400

DUNGEONS@DEFCON

A puzzling campaign for 1-4 players.

20 08 05 18 05 19 20 18 05

01 19 21 18 05 09 14 20 08

05 04 21 14 07 05 15 14 19

02 05 12 15 23 04 05 06 03

15 14 01 19 19 05 13 02 12

05 25 15 21 18 16 01 18 20

25 01 14 04 06 09 14 04 21

19

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000

EFF TECH TRIVIA



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 Cup and EFF swag pack. The second and third place teams will also win great EFF gear.

Location: Contest Area Stage

Hours: Friday 1500-1700

Twitter: @eff

Website: <https://eff.org>

GEEKPWN



Started by KEEN - and the first in 2014, GeekPwn enables security geeks around the world to exchange their thoughts and research findings. As the international intelligence security community, GeekPwn

tries to create secure life with secure techniques. In GeekPwn, YOU are encouraged to exploit unknown vulnerabilities of the cyber world. And together, WE aim to help manufacturers develop their security systems and create a better world.

The most unique and extraordinary character of a GeekPwn attendee is his/her open-minding and rich variety of PWN.

Security researchers are welcomed to GeekPwn if they are able to take control or obtain data without authorization under reasonable, realistic conditions (without tampering, pre-installed Trojans or certain pre-granted privileges), and target software and protocols of mobile phones, smart devices, Internet of Things, new I/O modules (gesture capture, VR, AR, etc.), AI-featured modules and services (robots, visual recognition and voice recognition), etc.

Location: Contest Area

Website: <http://www.geekpwn.org>

THE GOLD BUG - CRYPTO & PRIVACY VILLAGE PUZZLE

Love puzzles? Need a place to exercise your classical and modern cryptography skills? This puzzle will keep you intrigued over the course of DEF CON. VF GUVF ERNY BE VF VG N TNZR?

Location: Crypto & Privacy Village

Website: <http://goldbug.cryptovillage.org>

HACK FORTRESS



Teams of 10 (4 Hackers + 6 TF2 players) will compete to score more points than their opponents during each match. The goal is simple: score more points than your competitors. How you do that is where the challenge comes in. The TF2 players will be frantically trying to kill, capture and win rounds against

the opposing TF2 players. At the same time, the hackers will be attempting to solve a variety of hacking challenges. As tasks are completed, credits in our 'hackconomy' are gained. These can be used to purchase effects to help your team or hinder your opponents in both hacking and TF2.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000

Twitter: @tf2shmoov

Website: <http://hackfortress.net>

Twitch: hackfortresstv

Reddit: /r/HackFortress

HACK THE PLAN[E]T

Hack the Plan[e]t Capture the Flag (CTF) contest will feature GRIMM's 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 18 emulated or real devices and over 40 vulnerabilities that have been staged as challenges. Each of the challenges are of varying levels to test a competitor's 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 Range to provide an additional testbed for more advanced challenges in critical infrastructure and ICS environments.

Location: ICS Village

Twitter: @ICS_Village

Website: <https://www.icsvillage.com>

MISSION SE IMPOSSIBLE



What is Mission SE Impossible (MSI)? Maybe the best way to describe it is if the Gringo Warrior Challenge had a baby with Ethan Hunt while getting some scotch soaked DNA

from the Human Hacker, it would give birth to Mission SE Impossible. Also, this baby could shoot lasers out of it's eyes.

With lock picking, hand cuffs, laser obstacle course, some ciphers, and safe cracking MSI quickly became extremely popular in the SE Village. Folks of all ages have signed up and competed in this event and are watched by an enthusiastic crowd who is always willing to help out.

Location: Social Engineering Village

Hours: Friday All Day

Twitter: @humanhacker

Website: <https://www.social-engineer.org/social-engineer-village/>

OPENCTF



"In OpenCTF, teams compete to solve hacking challenges in a wide variety of categories, including web, forensics, programming, cryptography and

reverse engineering. There will be challenges for all skill levels. If you've never played in a capture the flag contest before, please feel free to stop by anyway - we'll explain how it works and do what we can to set set up with a team. Optional preregistration, as well as some tips on what to bring and how to prepare, can be found at OpenCTF.com.

You must have at least one team member attending to play OpenCTF. Arrangements for non-local players are none of our business or concern."

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @open_ctf

Website: <http://openctf.com>

OSINT CTF

Comprised of people who are interested giving back to society by helping to find missing persons and/or who want to learn more about open source intelligence (OSINT) gathering. This attracts people such as computer enthusiasts, information security professionals, first responders and private investigators.

Location: Online Only

Rules: <https://www.tracelabs.org/2018/05/defcon-26-osint-ctf-contest-rules-description/>
Slack Channel: <https://tracelabs.slack.com>

POCKET PROTECTOR CONTEST

Put your pocket protector designs through the ultimate gauntlet designed specifically to measure the usability, security, and style of your pocket protector.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

RED ALERT ICS CTF



Red Alert ICS CTF is based on ICS test bed (simulation) so all participant can hack actual devices. There are altogether some scenarios with its own set of challenges and scores. Challenges are from Bypass Airgap, ICS protocols and PLC & HMI softwares, Forensics, and Cyber Incidents (including classic and basic challenge, reversing and web).

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Website: <https://www.facebook.com/nshc.redalert/>

THE SCHEMAVERSE CHAMPIONSHIP

The Schemaverse [skee-muh vurs] is a space battleground that lives inside a PostgreSQL database. Mine the hell

CONTESTS

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!

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @schemaverse

Website: <http://schemaverse.com>

SE CTF



The Social Engineering Capture the Flag, SECTF, returns for its 9th year! Contestants have to fight with their own fears to prove they can SE like the best of them.

The flagship social engineering event! The SECTF is a test of bravery AND brains. It pits human against corporate security, in a contest that places the spotlight on the dangers of vishing, all in a 5x5 glass booth for your viewing enjoyment.

Location: Social Engineering Village

Hours: All Day Friday & Saturday

Twitter: @humanhacker

Website: <https://www.social-engineer.org/social-engineer-village/>

SE CTF KIDS



The SECTF4Kids has become its own DEF CON event!! What is it?

We have created a series of activities and challenges that will involve things like critical thinking

exercises, ciphers, logic puzzles, memory puzzles, verbal and nonverbal challenges, pitting kids against kids in a test of endurance (and fun).

This year's theme will surely challenge your kids. Ages 6-12.

Location: Social Engineering Village

Hours: Friday All Day

Twitter: @humanhacker

Website: <https://www.social-engineer.org/social-engineer-village/>

SE CTF TEENS



We have created a series of activities and challenges that will involve things like critical thinking

exercises, ciphers, logic puzzles, memory puzzles, verbal and nonverbal challenges, pitting TEENS against TEENS in a test of endurance (and fun).

This year's theme will surely challenge your kids. Ages 13-17.

Location: Social Engineering Village

Hours: Saturday All Day

Twitter: @humanhacker

Website: <https://www.social-engineer.org/social-engineer-village/>

SOHOPELESSLY BROKEN



SOHOpelessly BROKEN.

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! Scan the network to find every device and exploit as many as you can over the weekend. The top three teams will be rewarded!

Zero-Day Contest - The Zero-Day contest is focused on the discovery and demonstration of new exploits (0-day vulnerabilities). This track relies on the judging of newly discovered attacks against connected embedded electronic devices. Devices that are eligible for the contest can be found at <https://www.sohopelesslybroken.com/contests.php#0day> and you can start submitting entries now! The winners who score the highest on their judged entries will be rewarded with cash prizes. Contestants will need to provide proof that they disclosed the vulnerability to the vendor.

Location: IOT Village

Hours: Friday 1000-1900, Saturday 1000-1900, Sunday 1000-1300

Twitter: @SOHObroken

Website: <http://www.sohopelesslybroken.com>

SPELL CHECK: THE HACKER SPELLING BEE

The year is 1983. Supplies and entertainment are both running low and the machines are closing in. Suddenly, a technical editor from the future appears with a security style guide from 2018 and challenges you to spell terms as they appear in the guide. Maybe this quaint ritual will warm the hearts of the robots and bring in a new era of understanding to this troubled world. You're confident you can make it past "asset" and "botnet," but you get a sinking feeling that in later rounds, capitalization is going to count too. The odds are against you, but it's the end of the world... you might as well go out in a blaze of glory.

Location: Contest Area Stage

Hours: TBA (Check Info Booth)

Website: <https://www.bishopfox.com/blog/2018/02/hello-world-introducing-the-bishop-fox-cybersecurity-style-guide/>

TELECHALLENGE



Let your fingers do the hacking on your touch-tone phone! Dive into the telephonic world with a challenge that will pit your wits against the complexities of phone

systems, and the people and companies that inhabit them. The TeleChallenge is an immersive environment where all you need to get started is your phone. To win you'll hack your way into, around, and through a myriad of phone-connected services. How do you start? How do you play? How do you win? Good questions! Set sail with the TeleChallenge!

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @telechallenge

TIN FOIL HAT CONTEST



What with aliens and the NSA, a hacker can't always tell who's listening (or who's transmitting...). Show us your skills by building a tin foil hat to shield your subversive thoughts. There are 2 categories: stock, and unlimited. The hat in each category that blocks the most signal will receive the

"Substance" award for that category. We all know that hacker culture is all about looking good, though, so a single winner will be selected from all submissions for "Style". Finally, a single overall winner will be selected from all combined categories for "Style and Substance".

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday: Contest Area Stage - 1200-1300, Contest Area Stage - 1200-1300

Twitter: @DC_Tin_Foil_Hat

Website: <http://www.psychoholics.org/tfh>

THE UNDERHANDED HOME AUTOMATION CONTEST

The Underhanded Home Automation Contest is a nod to the yearly Underhanded C Contest. In spirit it strives for a similar goal; maximum damage from the seemingly innocuous. The contest requires participants to exploit home automation (IoT) devices in novel and arguably detrimental ways.

The rules are simple:

1. Choose one of the selected devices.
2. Devise a novel, subtle, and fiendish way to exploit the device or its operation.
3. Execute your plan, and document your process.
4. Showcase your findings.

A panel of 5 judges will score submissions in a number categories. They include the following: Impact, Underhandedness, Novelty, & Complexity. The top scoring entries win and will be showcased and revered.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @UnderhandedIoT

VULSEC VULNERABLE IMAGE BUILDING CONTEST



Tired of traditional events? attendees have been asked to submit the most devious virtual images for this contest. We have something for every hacker from the most experienced to the wannabe n00bs. VulnSec provides an on-site Cyber Range for contestants to have their images

pwned by DEF CON attendees. So, bring your hacking tools or use our provided Kali images to participate in this unique "by hackers for hackers" event. Still not interesting enough? Stop by, check our schedule for scheduled time trials and special events. Come out, test your abilities and claim a spot on our scoreboard!

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Website: <http://vulnsec.net>

WARLOCK GAM3Z CTF

warl0ck gam3z CTF is a hands-on 24/7; throw-down, no-

holds-barred hacker competition focusing on areas of physical security, digital forensics, hacker challenges and whatever craziness our exploit team develops. This is an online framework so participants can access it regardless of where they are or what network they are connected to via laptop, netbook, tablet or phone.

Most challenges require participants to download something that pertains to the problem at hand and solve the challenge using whatever tools, techniques or methods they have available. There are a multitude of point gainers on and off the game board. Extra point gainers will randomly appear on the game board in the form of The Judge, Bonus Questions, Free Tokens, One Time Tokens, Movie Trivia Quotes, Scavenger Hunts (online and onsite), Lock Picking (onsite) and Flash Challenges. Be careful of the 50/50 Token which may add or subtract points to your score.

The game board contains a scoring area so participants can view current standings, as well as an embedded chat function for those that may want to taunt their competitors, or work with other participants as part of a team. There is always an onsite moderator to assist participants that may be experiencing issues as well.

CONTESTS

All events that occur on the game board are sent o to Twitter as they happen. These include items such as participants signing up, leader of the board changes, scoring updates and challenge updates. Additionally, our Facebook site will be populated with information regarding the challenge and the current state of events.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Twitter: @gam3z_inc

Website: <https://www.facebook.com/Gam3zInc>



WHOSE SLIDE IS IT ANYWAY?

"Whose Slide Is It

Anyway?" is an unholy union of improv comedy, hacking and slide deck sado-masochism.

Location: Contest Area

Hours:

Twitter: @ImprovHacker

Website: <http://improvhacker.com/>

WIRELESS CTF



The Wireless Village presents the Wireless Capture the Flag (WCTF). We cater to those who are new to this game and those who have been playing for

a long time. Each WCTF begins with a presentation on How to WCTF. We also have a resources page on our website that guides participants in their selection of equipment to bring.

Location: Wireless Village

Twitter: @wctf_us

Website: <http://www.wirelessvillage.ninja/wctf.html>

EVENTS

8TH DEFCON BIKE RIDE



www.cycleoverride.org

See at 6am Friday! @jp_bourget @gdead @heidishmoo.

Location:

Hours: Friday - 0600

Twitter: @cycle_override

Website: <http://cycleoverride.org>

DEAF CON MEET UP



Deafcon. We help to provide communication services and spaces for professionals to meet and network with others. Anyone can come and attend our meet up and hangout!

Location: Chill-out Lounge

Hours: Saturday 1200

Twitter: @_DEAFCON_

Website: <https://www.deafconinc.org/>

HACKER KARAOKE



Do you like to sing? Do you want to perform? Ever wanted to sing in front of others? Come on down to the 10th Annual Hacker Karaoke, DEFCON's on-site karaoke experience. You can

be a star, or if you don't want to be a star, you can also take pride in making an utter fool of yourself.

Location: Emperors BR Chillout

Hours: Friday 2000-0200, Saturday 2000-0200

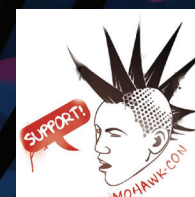
Twitter: @hackerkaraoke

Website: <https://hackerkaraoke.org/>

HAM RADIO EXAMS

Location: Anzio

MOHAWK-CON



Mohawk-Con returns for another year of shaving & coloring heads and transforming you into the cool kid at the con.

Charitable event to support the EFF & Hackers For Charity, get a cool new hawk in support of the causes that matter to you.

Location: Contest Area

Hours: Friday 1000-2000, Saturday 1000-2000, Sunday 1000-1200

Website: <https://www.facebook.com/MohawkCon/>

TOXIC BBQ



The humans of Vegas invite everyone to sear their meat in the searing heat! Kick off the con at Sunset Park, Pavilion F on Thursday afternoon with meat, beer, and conversation at this unofficial welcome party. Burgers and dogs are provided; contribute the rest as you can (more food, drinks, grilling, donations,

and rides). This event is off-site, so watch the Info Booth @dcib for carpool times and event updates.

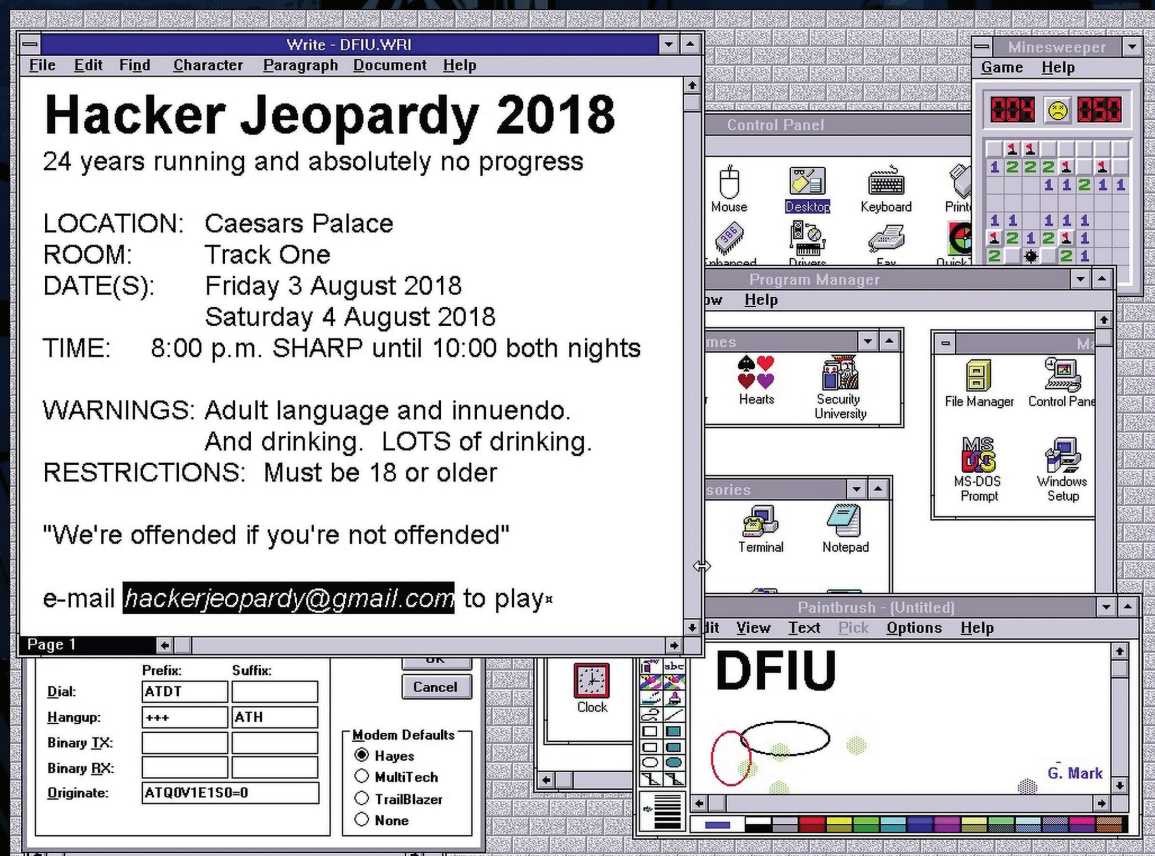
Location: Sunset Park, Pavilion F, (36.0636, -115.1178)

Hours: Thursday 1600-2200

LASER SHOOTING GALLERY

Experience the beauty of the Las Vegas area by shooting at inanimate objects with REAL lasers! Shoot aliens, robots, barrels and even cacti and try to get the high score. A presentation on how the gallery was conceived and constructed will occur Friday and Saturday at 3 PM in the shooting gallery room. Brought to you by the fine folks from Notacon.

Location: Venice, Caesars



PRESENTATIONS

Alpha by Speaker

DETECTING BLUE TEAM RESEARCH THROUGH TARGETED ADS

Saturday at 13:30 in Track 2
20 minutes

Ox200b
Hacker

When my implant gets discovered how will I know? Did the implant stop responding for some benign reason or is the IR team responding? With any luck they'll upload the sample somewhere public so I can find it, but what if I can find out if they start looking for specific bread crumbs in public data sources? At some point without any internal data all blue teams turn to OSINT which puts their searches within view of the advertising industry. In this talk I will detail how I was able to use online advertising to detect when a blue team is hot on my trail.

HACKING PLCS AND CAUSING HAVOC ON CRITICAL INFRASTRUCTURES

Saturday at 11:00 in 101 Track, Flamingo
45 minutes | Demo, Exploit

Thiago Alves
Ph.D. Student and Graduate Research Assistant at the University of Alabama in Huntsville

Programmable Logic Controllers (PLCs) are devices used on a variety of industrial plants, from small factories to critical infrastructures like nuclear power plants, dams and wastewater systems. Although PLCs were made robust to sustain tough environments, little care was taken to raise defenses against potential cyber threats. As a consequence, threats started pouring in and causing havoc. During this presentation I will talk about the architecture of a PLC and how it can be p0wned. There will be some live demonstration attacks against 3 different brands of PLCs (if the demo demons allow it, if not I will just show a video). Additionally, I will demonstrate two vulnerabilities I recently discovered, affecting the Rockwell MicroLogix 1400 series and the Schneider Modicon M221 controllers.

ASURA: A HUGE PCAP FILE ANALYZER FOR ANOMALY PACKETS DETECTION USING MASSIVE MULTITHREADING

Sunday at 13:30 in Track 1
20 minutes | Tool

Ruo Ando
Center for Cybersecurity Research and Development, National Institute of Informatics, Japan

Recently, the inspection of huge traffic log is imposing a great burden on security analysts. Unfortunately, there have been few research efforts focusing on scalability in analyzing very large PCAP file with reasonable computing resources. Asura is a portable and scalable PCAP file analyzer for detecting anomaly packets using massive multithreading. Asura's parallel packet dump inspection is based on task-based decomposition and therefore can handle massive threads for large PCAP file without considering tidy parameter selection in adopting data decomposition. Asura is designed to scale out in processing large PCAP file by taking as many threads as possible.

Asura takes two steps. First, Asura extracts feature vector represented by associative containers of <sourceIP, destIP> pair. By doing this, the feature vector can be drastically small compared with the size of original PCAP files. In other words, Asura can reduce packet dump data into the size of unique <sourceIP, destIP> pairs (for example, in experiment, Asura's output which is reduced in first step is about 2% compared with the size of original libpcap files). Second, a parallel clustering algorithm is applied for the feature vector which is represented as {<sourceIP, destIP>, V[i]} where V[i] is aggregated flow vector. In second step, Asura adopts an enhanced Kmeans algorithm. Concretely, two functions of Kmeans which are (1)calculating distance and (2)relabeling points are improved for parallel processing.

In experiment, in processing public PCAP datasets, Asura can identified 750 packets which are labeled as malicious from among 70 million (about 18GB) normal packets. In a nutshell, Asura successfully found

750 malicious packets in about 18GB packet dump. For Asura to inspect 70 million packets, it took reasonable computing time of around 350-450 minutes with 1000-5000 multithreading by running commodity workstation. Asura will be released under MIT license and available at author's GitHub site on the first day of DEF CON 26.

ONE BITE AND ALL YOUR DREAMS WILL COME TRUE: ANALYZING AND ATTACKING APPLE KERNEL DRIVERS

Sunday at 14:00 in Track 3
45 minutes | Demo, Tool, Exploit

Xiaolong Bai
Security Engineer, Alibaba Inc.

Min (Spark) Zheng
Security Expert, Alibaba Inc.

Though many security mechanisms are deployed in Apple's macOS and iOS systems, some old-fashioned or poor-quality kernel code still leaves the door widely open to attackers. Especially, as kernel's critical components, device drivers are frequently exploited to attack Apple systems. In fact, bug hunting in Apple kernel drivers is not easy since they are mostly closed-source and heavily relying on object-oriented programming. In this talk, we will share our experience of analyzing and attacking Apple kernel drivers. In specific, we will introduce a new tool called Ryuk. Ryuk employs static analysis techniques to discover bugs by itself or assist manual review.

In addition, we further combine static analysis with dynamic fuzzing for bug hunting in Apple drivers. In specific, we will introduce how we integrate Ryuk to the state-of-art Apple driver fuzzer, PassiveFuzzFrameworkOSX, for finding exploitable bugs.

Most importantly, we will illustrate Ryuk's power with several new vulnerabilities that are recently discovered by Ryuk. In specific, we will show how we exploit these vulnerabilities for privilege escalation on macOS 10.13.3 and 10.13.2. We will not only explain why these bugs occur and how we find them, but also demonstrate how we exploit them with innovative kernel exploitation techniques.

YOU MAY HAVE PAID MORE THAN YOU IMAGINE: REPLAY ATTACKS ON ETHEREUM SMART CONTRACTS

Saturday at 10:00 in Track 3
45 minutes | Demo, Exploit

Zhenxuan Bai
Freelance Security Researcher

Yuwei Zheng
Senior Security Researcher, Unicorn Team, 360 Technology

Senhua Wang
Freelance Security Researcher

Kunzhe Chai
Leader of PegasusTeam at 360 Radio Security Research Department, 360 Technology

In this paper, a new replay attack based on Ethereum smart contracts is presented. In the token transfer, the risk of replay attack cannot be completely avoided when the sender's signatures are abused, which can bring the loss to users. And the reason is that the applying scope of the signatures is not properly designed in the smart contracts. To test and verify this loophole, we selected two similar smart contracts for our experiment, at the same time, we used our own accounts in these two contracts to carry out the experiment. Because the same signatures of the two contracts were used in the experiment, we got a double income from sender successfully. The experiment verified that the replay attack is really exist. Besides, the replay attack may exist in multiple smart contracts. We calculated the number of smart contracts with this loophole, as well as the corresponding transaction activities, which find some Ethereum smart contracts are risked for this loophole. According to the vulnerability of the contract signature, the risk level is calibrated and depicted. Furthermore, the replay attack pattern is extended to within contract, cross contract and cross chain, which provide the pertinence and well reference for protection. Finally, the countermeasures are proposed to fix this vulnerability.

WHAT THE FAX!?

Sunday at 15:00 in Track 2
45 minutes | Demo, Tool, Exploit, Audience Participation

Yaniv Balmas
Security Researcher, Check Point Software Technologies

Eyal Itkin
Security Researcher, Check Point Software Technologies

Unless you've been living under a rock for the past 30 years or so, you probably know what a fax machine is. For decades, fax machines were used worldwide as the main way of electronic document delivery. But this happened in the 1980s. Humanity has since developed far more advanced ways to send digital content, and fax machines are all in the past, right? After all, they should now be nothing more than a glorified museum item. Who on earth is still using fax machines?

The answer, to our great horror, is EVERYONE. State authorities, banks, service providers and many others are still using fax machines, despite their debatable quality and almost non-existent security. In fact, using fax machines is often mandatory and considered a solid and trustworthy method of delivering information.

What the Fax?! We embarked on a journey with the singular goal of disrupting this insane state of affairs. We went to work, determined to show that the common fax machine could be compromised via mere access to its fully exposed and unprotected telephone line—thus completely bypassing all perimeter security protections and shattering to pieces all modern-day security concepts.

Join us as we take you through the strange world of embedded operating systems, 30-year-old protocols, museum grade compression algorithms, weird extensions and undebuggable environments. See for yourself first-hand as we give a live demonstration of the first ever full fax exploitation, leading to complete control over the entire device as well as the network, using nothing but a standard telephone line.

This talk is intended to be the canary in the coal mine. The technology community cannot

sit idly by while this ongoing madness is allowed to continue. The world must stop using FAX!

ROCK APPROUND THE CLOCK: TRACKING MALWARE DEVELOPERS BY ANDROID "AAPT" TIMEZONE DISCLOSURE BUG

Sunday at 10:00 in Track 1
45 minutes | Demo

Sheila A. Berta
Security Researcher at Eleven Paths

Sergio De Los Santos
Head of Innovation and Lab at Eleven Paths

Are you a malware developer for Android devices? We have very bad news for you: the Android-SDK packager (aapt) is leaking your time zone! We have found a bug inside this Android-SDK's component that relies in not properly setting the value of a variable used as an argument for localtime() function, when setting the "Last Modified" field for the Android App's files. Because of this, the time zone of anyone using the Android-SDK packager to generate their APKs is leaked. The curious thing is that, despite of this bug inside aapt, the problem goes even beyond aapt itself: its roots goes deep into an incorrect handling errors in the operative system functions localtime() (Windows) and localtime_r() (UNIX).

Because of in the world of Threat Intelligence determining the attacker's geographical location of is one of the most valuable data for attribution techniques, we focused our research in taking advantage of this bug for tracking Android malware developers. In addition to this, we have discovered another very effective way to find out the developer's time zone, based on a calculation of times extracting the GMT timestamp from the Android's app files and the UTC timestamp of the self-signed,"disposable" certificate added to the application (most common cases in malware developers). This is what we call: Rock appround the clock! Using these two different techniques, we have crunched some numbers with our 10 million apps database to determine how these leaked time zones (with one or another technique) are related with malware and which

PRESENTATIONS

are the countries that generate more Android malicious applications, what is the possible relation between time zone and “malware likelihood” among other interesting numbers.

But that’s not all, we have another bad news for malware developers: no IDE (even Android Studio) removes metadata from the files added to the Android app. We will show examples with real cases in which, after analyzing the metadata of files inside the .apk, we got to know country, language, or even more specific geographical location of the developer and -in some cases- the name of the suppose-to-be-anonymous developer! Finally, we will share the scripts we have built to get all this information with just a simple click.

RING 0/-2 ROOTKITS: BYPASSING DEFENSES

Thursday at 12:00 in 101 Track, Flamingo
45 minutes

Alexandre Borges
Malware and Security Researcher at Blackstorm Security

Advanced malware such as TDL4, Rovnix, Gapz, Omasco, Mebromi and others have exposed in recent years various techniques used to circumvent the usual defenses and have shown how much companies are not prepared to deal with these sophisticated threats.

Although the industry has implemented new protections such as Virtualized Based Security, Windows SMM Security Mitigation Table (WSMT), Kernel Code Signing, HVCI, ELAM, Secure Boot, Boot Guard, BIOS Guard, and many others, it is still unknown the professionals of the architecture of these protections, what are the components attacked by these contemporary malwares in the context of BIOS / UEFI and what are the tricks used by them. Precisely because of the lack of adequate understanding, most machines (BIOS / UEFI + operating system) remain vulnerable in the same way as a few years ago.

In addition, there are a growing number of malwares that have used kernel drivers to circumvent limitations and protections in order to gain full access to the operating

system and data. Exactly for these reasons, it is necessary to understand the way that malwares act as device drivers and what are the mechanisms used by these threats to infect an operating system.

The purpose of this presentation is to show clearly and without too much details that often hinders understanding, how these threats act, which components are attacked, what are the techniques used by these advanced malware to subvert the system and how existing protections work.

TROUBLE IN THE TUBES: HOW INTERNET ROUTING SECURITY BREAKS DOWN AND HOW YOU CAN DO IT AT HOME

Sunday at 13:00 in 101 Track, Flamingo
45 minutes | Demo, Tool

Lane Broadbent
Security Engineer, Vivint

We all protect our home networks, but how safe is your data once it leaves on its journey to the latest cat pictures? How does your traffic make it to its destination and what threats does it face on its way? What is BGP and why should you care?

In this talk, I’ll explain the basic structure of the network that is the Internet and the trust relationships on which it is built. We’ll explore several types of attacks that you may have seen in the news that exploit this relationship to bring down websites, steal cryptocurrency, and monitor dissidents.

Because talking about bringing down the Internet isn’t as much fun as doing, I’ll show how to create a mini Internet using Mininet and demonstrate the attacks without the need for a BGP router or a lawyer. Finally, because nation states shouldn’t get to have all the fun, I’ll use Scapy and some novel techniques to demonstrate how a compromised router can be used to prevent attribution, frame a friend, or create a covert communication channel.

LAST MILE AUTHENTICATION PROBLEM: EXPLOITING THE MISSING LINK IN END-TO-END SECURE COMMUNICATION

Sunday at 12:00 in Track 1
45 minutes | Demo, Exploit

Thanh Bui
Security Researcher, Aalto University, Finland

Siddharth Rao
Security Researcher, Aalto University, Finland

With “Trust none over the Internet” mindset, securing all communication between a client and a server with protocols such as TLS has become a common practice. However, while the communication over Internet is routinely secured, there is still an area where such security awareness is not seen: inside individual computers, where adversaries are often not expected.

This talk discusses the security of various inter-process communication (IPC) mechanisms that local processes and applications use to interact with each other. In particular, we show IPC-related vulnerabilities that allow a non-privileged process to steal passwords stored in popular password managers and even second factors from hardware tokens. With passwords being the primary way of authentication, the insecurity of this “last mile” causes the security of the rest of the communication strands to be obsolete. The vulnerabilities that we demonstrate can be exploited on multi-user computers that may have processes of multiple users running at the same time. The attacker is a non-privileged user trying to steal sensitive information from other users. Such computers can be found in enterprises with centralized access control that gives multiple users access to the same host. Computers with guest accounts and shared computers at home are similarly vulnerable.

REVERSE ENGINEERING WINDOWS DEFENDER’S EMULATOR

Saturday at 15:00 in Track 2
45 minutes | Demo, Tool

Alexei Bulazel
Hacker

Windows Defender Antivirus’s mpengine.dll implements the core of Defender’s functionality in an enormous ~11 MB, 30,000+ function DLL.

In this presentation, we’ll look at Defender’s emulator for analysis of potentially malicious Windows binaries on the endpoint. To the best of my knowledge, there has never been a conference talk or publication on reverse engineering any antivirus binary emulator before.

We’ll cover a range of topics including emulator internals—machine code to intermediate language translation and execution; memory management; Windows API emulation; NT kernel emulation; file system and registry emulation; integration with Defender’s antivirus features; the virtual environment; etc.—building custom tooling for instrumenting the emulator; tricks that binaries can use to evade or subvert analysis; and attack surface within the emulator.

Attendees will leave with an understanding of how modern antivirus software conducts emulation-based dynamic analysis on the endpoint, and how attackers might go about subverting or attacking these systems. I’ll publish code for a binary for exploring the emulator from within, patches that I developed for instrumenting Defender built on top of Tavis Ormandy’s loadlibrary project, and IDA scripts to help with analyzing mpengine.dll and Defender’s “VDLLs”.

A JOURNEY INTO HEXAGON: DISSECTING A QUALCOMM BASEBAND

Thursday at 13:00 in 101 Track, Flamingo
45 minutes

Seamus Burke
Hacker

Mobile phones are quite complicated and feature multiple embedded processors handling wifi, cellular connectivity, bluetooth, and other signal processing in addition to the application processor. Have you ever been curious about how your phone actually makes calls and texts on a low level? Or maybe you want to learn more about the internals of the baseband but have no clue where to

start. We will dive into the internals of a qualcomm baseband, tracing it’s evolution over the years until its current state. We will discuss the custom, in-house DSP architecture they now run on, and the proprietary RTOS running on it. We will also cover the architecture of the cellular stack, likely places vulnerabilities lie, and exploit mitigations in place. Finally we will cover debugging possibilities, and how to get started analyzing the baseband firmware—how to differentiate between RTOS and cellular functions, how to find C std library functions, and more.

RELOCATION BONUS: ATTACKING THE WINDOWS LOADER MAKES ANALYSTS SWITCH CAREERS

Saturday at 17:00 in Track 2
45 minutes | Demo, Tool

Nick Cano
Senior Security Architect @ Cylance

The arbiters of defense wield many static analysis tools; disassemblers, PE viewers, and anti-viruses are among them. When you peer into their minds, these tools reveal their perilous implementations of PE file parsing. They assume PE files come as-is, but the Windows Loader actually applies many mutations (some at the command of the PE itself) before execution ever begins. This talk is about bending that loader to one’s whim with the Relocations Table as a command spell. It will demonstrate how the loader can be instrumented into a mutation engine capable of transforming an utterly mangled PE file into a valid executable. This method starts with multiple ASLR Preselection attacks that force binary mapping at a predictable address. It then mangles the PE file, garbling any byte not required prior to relocation. Finally, it embeds a new Relocations Table which, when paired with a preselected base address, causes the loader to reconstruct the PE and execute it with ease. This isn’t a packer or a POC, it is a PE rebuilder which generates completely valid, stable, and vastly tool-breaking executables. This talk will show you how this attack twists the protocols of a machine against

the controls meant to protect it. It flexes on tools with various look-what-I-can-break demonstrations and, if you write similar tools, it’ll make you rethink how you do it.

PROJECT INTERCEPTOR: AVOIDING COUNTER-DRONE SYSTEMS WITH NANODRONES

Saturday at 15:00 in 101 Track, Flamingo
45 minutes | Demo, Tool, Audience Participation

David Melendez Cano
R&D Embedded Systems Engineer. Albalá Ingenieros S.A.

Antidrone system industries have arisen. Due to several, and even classic, vulnerabilities in communication systems now used by drones, anti-drone systems are able to take down those drones by means of well documented attacks.

Drone/antidrone competition has already been set into the scene. This talk provides a new vision about drone protection against anti-drone systems, presenting “The Interceptor Project”, a hand-sized nano drone based on single-core tiniest Linux Board: Vocore2.

This Linux board manages a WiFi (side/hidden) bidirectional channel communication that cannot be deauthenticated and it is replay-resistant, keeping all 802.11 hacking capabilities and standard utilities as any other WiFi hacker drone, with only the built-in adapter of the tiny Vocore2. Also, a “just in case”, fallback control by SDR is implemented taking advantage of all the goods that SDR radio gives. All embedded into a hand-sized aircraft to make detection and mitigation a real and new pain, with a very low budget: About \$70.

YOU’D BETTER SECURE YOUR BLÉ DEVICES OR YOU’LL KICK YOUR BUTTS!

Saturday at 12:00 in Track 2
45 minutes | Demo, Tool, Exploit

Damien “virtualabs” Cauquil
Head of Research & Development, Digital Security

Sniffing and attacking Bluetooth Low Energy devices has always been a real pain. Proprietary tools do the job but cannot be tuned

PRESENTATIONS

to fit our offensive needs, while opensource tools work sometimes, but are not reliable and efficient. Even the recently released Man-in-the-Middle BLE attack tools have their limits, like their complexity and lack of features to analyze encrypted or short connections.

Furthermore, as vendors do not seem inclined to improve the security of their devices by following the best practices, we decided to create a tool to lower the ticket: BtleJack. BtleJack not only provides an affordable and reliable way to sniff and analyze Bluetooth Low Energy devices and their protocol stacks, but also implements a brand new attack dubbed “BtleJacking” that provides a way to take control of any already connected BLE device.

We will demonstrate how this attack works on various devices, how to protect them and avoid hijacking and of course release the source code of the tool.

Vendors, be warned: BLE hijacking is real and should be considered in your threat model.

BUILDING THE HACKER TRACKER

Thursday at 15:00 in 101 Track, Flamingo
20 minutes

Whitney Champion
Senior Systems Engineer

Seth Law
Application Security Consultant, Redpoint Security

In 2012, back when DEF CON still fit in the Riviera (RIP), I recognized a gap to fill. I wanted to create a mobile version of the paper DEF CON booklet that everyone could use at the con.

I was unable to attend the conference that year. I was 8 months pregnant with my first child, and because I couldn't be there in person, I spent a lot of time wishing I was.

So I built it. I spent countless hours pouring my heart into what became the Hacker Tracker, shiny graphics and all, and was committing code up until the minute I went into labor.

Fast forward a few years: Seth was frustrated with the lack of a mobile app for iOS while attending DEF CON. Subsequently, he found the

Android version of Hacker Tracker and reached out to me about creating an iOS version. I was thrilled that someone wanted to join me and help grow the project. Not long after that, I recruited Chris to work on the app as well.

Now, 6 years since its inception, a small team supports the app development across iOS and Android and the apps are being used by half a dozen different conferences, representing several thousand users.

From nothing to something, we've experienced quite a bit in 6 years. Join us as we share our moments of joy, fear, and panic, "things not to do", and more.

DEF CON CLOSING CEREMONIES

Sunday at 16:00 in Track 1
105 minutes | Audience Participation

The Dark Tangent

DEF CON Closing Ceremonies

OUTSMARTING THE SMART CITY

Saturday at 16:00 in 101 Track, Flamingo
45 minutes | Demo, Exploit

Daniel “unicornFurnace” Crowley
Research Baron, IBM X-Force Red

Mauro Paredes
Hacker

Jen “savagejen” Savage
Hacker

The term “smart city” evokes imagery of flying cars, shop windows that double as informational touchscreens, and other retro-futuristic fantasies of what the future may hold. Stepping away from the smart city fantasy, the reality is actually much more mundane. Many of these technologies have already quietly been deployed in cities across the world. In this talk, we examine the security of a cross-section of smart city devices currently in use today to reveal how deeply flawed they are and how the implications of these vulnerabilities could have serious consequences.

In addition to discussing newly discovered pre-auth attacks against multiple smart city devices from different categories of smart city technology, this presentation will discuss methods for how to

figure out what smart city tech a given city is using, the privacy implications of smart cities, the implications of successful attacks on smart city tech, and what the future of smart city tech may hold.

DEF CON 101 PANEL

Thursday at 15:30 in 101 Track, Flamingo
105 minutes | Audience Participation

HighWiz
Founder, DC 101

Nikita
Director of Content & Coordination, DEF CON

Roamer
CFP Vocal Antagonizer

Chris “Suggy” Sumner
Co-Founder, Online Privacy Foundation

Jericho
“Squirrel”

Wiseacre
Former Doer Of Things

Shaggy
The Mountain

Ten years ago, DEF CON 101 was founded by HighWiz as a way to introduce n00bs to DEF CON. The idea was to help attendees get the best experience out of DEF CON (and also tell them how to survive the weekend!). The DEF CON 101 panel has been a way for people who have participated in making DEF CON what it is today to share those experiences and, hopefully, inspire attendees to expand their horizons. DEF CON offers so much more than just talks and the DEF CON 101 panel is the perfect place to learn about all things DEF CON so you, dear reader, can get the best experience possible. The panel will end with the time honored tradition of “Name the n00b” where lucky attendees will be brought up on stage to introduce themselves to you and earn the coveted 101 n00b handle. Don't worry if you don't make it on to the stage, there will be plenty of other prizes for you to enjoy!

DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

Friday at 20:00-22:00 in Octavius 9
Fireside Hax

Christian “quaddi” Dameff MD
Emergency physician, Clinical Informatics fellow at The University of California San Diego.

Jeff “r3plicant” Tully MD
Pediatrician, Anesthesiologist, University of California Davis

Kirill Levchenko PhD
Associate Professor of Computer Science, University of California San Diego

Beau Woods
Hacker

Roberto Suarez
Hacker

Jay Radcliffe
Hacker

Joshua Corman
Hacker

David Nathans
Hacker

Healthcare cybersecurity is in critical condition. That's not FUD, that's the bottom line from the Congressionally mandated Health Care Industry Cybersecurity Task Force report released just last year, a year which also saw the twin specters of WannaCry and NotPetya take down entire hospital systems while over half a million implanted pacemakers were recalled in the fallout of one of the most (ir)responsible disclosures in recent memory. It's enough to make any concerned white hat reach for a stiff drink. And that's where we come in. After an incredibly successful, near-fire-code-violating jam packed session at DC25 as an Evening Lounge, ‘D0 N0 H4rm’ is diving deeper and going longer as it transforms into a Fireside Hax, assembling an even larger and more distinguished panel of expert hackers, policymakers, wonks, and health care providers to continue discussing, dissecting, and most importantly, debating the ways to keep patients safe in an increasingly perilous space. Featuring continuous audience interaction and with the same loose and informal flow that characterized the initial, libation rich hotel room gatherings, moderators quaddi and r3plicant invite you to add your voice to this incredibly important conversation. Pin this one down quickly, pre-registration is going to go fast.

YOUR BANK'S DIGITAL SIDE DOOR

Friday at 17:00 in 101 Track, Flamingo
45 minutes | Demo, Tool

Steven Danneman
Security Engineer, Security Innovation

Why does my bank's website require my MFA token but Quicken sync does not? How is using Quicken or any personal financial software different

from using my bank's website? How are they communicating with my bank? These questions ran through my head when balancing the family checkbook every month.

Answering these questions led me to deeply explore the 20 year old Open Financial Exchange (OFX) protocol and the over 3000 North American banks that support it. They led me to the over 30 different implementations running in the wild and to a broad and inviting attack surface presented by these banks' digital side doors.

Now I'd like to guide you through how your Quicken, QuickBooks, Mint.com, or even GnuCash applications are gathering your checking account transactions, credit card purchases, stock portfolio, and tax documents. We'll watch them flow over the wire and learn about the jumble of software your bank's IT department deploys to provide them. We'll discuss how secure these systems are, that keep track of your money, and we'll send a few simple packets at several banks and count the number of security WTFs along the way.

Lastly, I'll demo and release a tool that fingerprints an OFX service, describes its capabilities, and assesses its security.

PANEL: DEF CON GROUPS

Sunday at 15:00 in Track 1
45 minutes | Audience Participation

Brent White (BITKILL3R)
DEF CON Groups Global Coordinator

Jeff Moss (The Dark Tangent)
Founder, DEF CON

Jayson E. Street
DEF CON Groups Global Ambassador

SOups

Tim Roberts (byt3boy)

Casey Bourbonnais

April Wright

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 special event, your DEF CON groups team who works behind the scenes to make DCG

possible will introduce themselves and provide status updates. After we're done talking, the remainder of time will be an informal open floor right there in the room to mingle and talk all things DCG.

There will be a:

- Designated area in the room for those wanting to start/join a group

- Designated area in the room for those wanting to share project ideas

YOUR VOICE IS MY PASSPORT

Friday at 16:00 in Track 3
45 minutes | Demo, Exploit

_delta_zero
Senior Data Scientist, Salesforce

Azeem Aqil
Senior Security Software Engineer, Salesforce

Financial institutions, home automation products, and offices near universal cryptographic decoders have increasingly used voice fingerprinting as a method for authentication. Recent advances in machine learning and text-to-speech have shown that synthetic, high-quality audio of subjects can be generated using transcribed speech from the target. Are current techniques for audio generation enough to spoof voice authentication algorithms? We demonstrate, using freely available machine learning models and limited budget, that standard speaker recognition and voice authentication systems are indeed fooled by targeted text-to-speech attacks. We further show a method which reduces data required to perform such an attack, demonstrating that more people are at risk for voice impersonation than previously thought.

THE RING O FA ADE: AWAKENING THE PROCESSOR'S INNER DEMONS

Saturday at 13:30 in Track 1
20 minutes | Demo, Tool

Christopher Domas
Director of Research, Finite State

Your computer is not yours. You may have shelled out thousands of dollars for it. It may be sitting right there on your desk. You may have carved your name deep into its side with a

PRESENTATIONS

blowtorch and chisel. But it's still not yours. Some vendors are building secret processor registers into your system's hardware, only accessible by shadowy third parties with trusted keys. We as the end users are being intentionally locked out and left in the dark, unable to access the heart of our own processors, while select organizations are granted full control of the internals of our CPUs. In this talk, we'll demonstrate our work on how to probe for and unlock these previously invisible secret registers, to break into all-powerful features buried deep within the processor core, to finally take back our own computers.

GOD MODE UNLOCKED: HARDWARE BACKDOORS IN [REDACTED] X86 CPUS

Friday at 14:00 in Track 1
45 minutes | Demo, Tool, Exploit

Christopher Domas
Director of Research, Finite State

Complexity is increasing. Trust eroding. In the wake of Spectre and Meltdown, when it seems that things cannot get any darker for processor security, the last light goes out. This talk will demonstrate what everyone has long feared but never proven: there are hardware backdoors in some x86 processors, and they're buried deeper than we ever imagined possible. While this research specifically examines a third-party processor, we use this as a stepping stone to explore the feasibility of more widespread hardware backdoors.

ONE-LINERS TO RULE THEM ALL

Friday at 11:00 in Track 2
45 minutes | Demo

egypt
Security Analyst, Black Hills Information Security

William Vu
Security Researcher, Rapid7

It began with the forging of the command line. And some things that should not have been forgotten, were lost. History became legend, legend became myth.

Sometimes you just need to pull out the third column of a CSV file. Sometimes you just need to sort IP addresses. Sometimes you have to pull out IP addresses from the third

column and sort them, but only if the first column is a particular string and for some reason the case is random.

In this DEF CON 101 talk, we'll cover a ton of bash one-liners that we use to speed up our hacking. Along the way, we'll talk about the concepts behind each of them and how we apply various strategies to accomplish whatever weird data processing task comes up while testing exploits and attacking a network.

LOST AND FOUND CERTIFICATES: DEALING WITH RESIDUAL CERTIFICATES FOR PRE-OWNED DOMAINS

Sunday at 13:30 in Track 2
20 minutes | Demo, Tool

Ian Foster
Hacker

Dylan Ayrey
Hacker

When purchasing a new domain name you would expect that you are the only one who can obtain a valid SSL certificate for it, however that is not always the case. When the domain had a prior owner(s), even several years prior, they may still possess a valid SSL certificate for it and there is very little you can do about it.

Using Certificate Transparency, we examined millions of domains and certificates and found thousands of examples where the previous owner for a domain still possessed a valid SSL certificate for the domain long after it changed ownership. We will review the results from our ongoing large scale quantitative analysis over past and current domains and certificates. We'll explore the massive scale of the problem, what we can do about it, how you can protect yourself, and a proposed process change to make this less of a problem going forwards.

We end by introducing BygoneSSL, a new tool and dashboard that shows an up to date view of affected domains and certificates using publicly available DNS data and Certificate Transparency logs. BygoneSSL will demonstrate how widespread the issue is, let domain owners determine if

they could be affected, and can be used to track the number of affected domains over time.

DEFENDING THE 2018 MIDTERM ELECTIONS FROM FOREIGN ADVERSARIES

Sunday at 10:00 in Track 2
45 minutes | Demo, Tool

Joshua M. Franklin
Hacker

Kevin Franklin
Hacker

Election Buster is an open source tool created in 2014 to identify malicious domains masquerading as candidate webpages and voter registration systems. During 2016, fake domains were used to compromise credentials of a Democratic National Committee (DNC) IT services company, and foreign adversaries probed voter registration systems. The tool now cross-checks domain information against open source threat intelligence feeds, and uses a semi-autonomous scheme for identifying phundraising and false flag sites via ensembled data mining and deep learning techniques. We identified Russian nationals registering fake campaign sites, candidates deploying defensive—and offensive—measures against their opponents, and candidates unintentionally exposing sensitive PII to the public. This talk provides an analysis of our 2016 Presidential Election data, and all data recently collected during the 2018 midterm elections. The talk also details technological and procedural measures that government offices and campaigns can use to defend themselves.

FOR THE LOVE OF MONEY: FINDING AND EXPLOITING VULNERABILITIES IN MOBILE POINT OF SALES SYSTEMS

Sunday at 10:00 in Track 3
45 minutes | Demo, Tool

Leigh-Anne Galloway
Cyber Security Resilience Lead, Positive Technologies

Tim Yunusov
Hacker

These days it's hard to find a business that doesn't accept faster

payments. Mobile Point of Sales (mPOS) terminals have propelled this growth lowering the barriers for small and micro-sized businesses to accept non-cash payments. Older payment technologies like mag-stripe still account for the largest majority of all in-person transactions. This is complicated further by the introduction of new payment standards such as NFC. As with each new iteration in payment technology, inevitably weaknesses are introduced into this increasingly complex payment eco-system.

In this talk, we ask, what are the security and fraud implications of removing the economic barriers to accepting card payments; and what are the risks associated with continued reliance on old card standards like mag-stripe? In the past, testing for payment attack vectors has been limited to the scope of individual projects and to those that have permanent access to POS and payment infrastructure. Not anymore!

In what we believe to be the most comprehensive research conducted in this area, we consider four of the major mPOS providers spread across the US and Europe; Square, SumUp, iZettle and Paypal. We provide live demonstrations of new vulnerabilities that allow you to MitM transactions, send arbitrary code via Bluetooth and mobile application, modify payment values for mag-stripe transactions, and a vulnerability in firmware; DoS to RCE. Using this sampled geographic approach, we are able to show the current attack surface of mPOS and, to predict how this will evolve over the coming years.

For audience members that are interested in integrating testing practices into their organization or research practices, we will show you how to use mPOS to identify weaknesses in payment technologies, and how to remain undetected in spite of anti-fraud and security mechanisms.

PRESENTATIONS

IT'S ASSEMBLER, JIM, BUT NOT AS WE KNOW IT: (AB)USING BINARIES FROM EMBEDDED DEVICES FOR FUN AND PROFIT

Friday at 12:00 in 101 Track, Flamingo
45 minutes | Demo

Morgan "indrora" Gangwere
Hacker

With the proliferation of Linux-based SoCs—you've likely got one or two in your house, on your person or in your pocket—it is often useful to look "under the hood" at what is running; Additionally, in-situ debugging may be unavailable due to read-only filesystems, memory is often limited, and other factors keep us from attacking a live device. This talk looks at attacking binaries outside their native environment using QEMU, the Quick Emulator, as well as techniques for extracting relevant content from devices and exploring them.

PLAYBACK: A TLS 1.3 STORY

Friday at 15:00 in Track 2
45 minutes | Demo

Alfonso Garcia Alguacil
Senior Penetration Tester, Cisco

Alejo Murillo Moya
Red Team Lead EMEAR, Cisco

TLS 1.3 is the new secure communication protocol that should be already with us. One of its new features is 0-RTT (Zero Round Trip Time Resumption) that could potentially allow replay attacks. This is a known issue acknowledged by the TLS 1.3 specification, as the protocol does not provide replay protections for 0-RTT data, but proposed countermeasures that would need to be implemented on other layers, not at the protocol level. Therefore, the applications deployed with TLS 1.3 support could end up exposed to replay attacks depending on the implementation of those protections.

This talk will describe the technical details regarding the TLS 1.3 0-RTT feature and its associated risks. It will include Proof of Concepts (PoC) showing real-world replay attacks against TLS 1.3 libraries and browsers. Finally, potential solutions or mitigation controls

would be discussed that will help to prevent those attacks when deploying software using a library with TLS 1.3 support.

HAVING FUN WITH IOT: REVERSE ENGINEERING AND HACKING OF XIAOMI IOT DEVICES

Saturday at 14:00 in 101 Track, Flamingo
45 minutes | Demo, Tool, Exploit

Dennis Giese
Hacker

While most IoT accessory manufacturers have a narrow area of focus, Xiaomi, an Asian based vendor, controls a vast IoT ecosystem, including smart lightbulbs, sensors, cameras, vacuum cleaners, network speakers, electric scooters and even washing machines. In addition, Xiaomi also manufactures smartphones. Their products are sold not only in Asia, but also in Europe and North America. The company claims to have the biggest IoT platform worldwide.

In my talk, I will give a brief overview of the most common, Wi-Fi based, Xiaomi IoT devices. Their devices may have a deep integration in the daily life (like vacuum cleaners, smart toilet seats, cameras, sensors, lights).

I will focus on the features, computational power, sensors, security and ability to root the devices. Let's explore how you can have fun with the devices or use them for something useful, like mapping Wi-Fi signal strength while vacuuming your house. I will also cover some interesting things I discovered while reverse engineering Xiaomi's devices and discuss which protections were deployed by the developers (and which not).

Be prepared to see the guts of many of these devices. We will exploit them and use them to exploit other devices.

PRESENTATIONS

BEYOND THE LULZ: BLACK-HAT TROLLING, WHITE-HAT TROLLING, ATTACKING AND DEFENDING OUR ATTENTION LANDSCAPE

Saturday at 20:00-22:00 in Octavius 9
Fireside Hax

Matt Goerzen
Researcher, Data & Society

Dr. Jeanna Matthews
Fellow at Data & Society, Associate Professor of
Computer Science at Clarkson University

Joan Donovan
Media Manipulation/Platform Accountability Research
Lead, Data and Society in Manhattan

White hat or critical grey hat trolling? Trolling as art? Trolling as hybrid warfare? Trolling as propaganda? In this Fireside Hax, we will challenge your assumptions about trolling. Trolls are attention hackers, using social and technical means to bait journalists, set agendas, game media gatekeepers, and direct audiences. Sometimes they also have fun. We will discuss a range of trolling techniques like sockpuppeting, dogpiling, doxing, attention honeypots, and cognitive denial of service attacks that we have not seen concisely catalogued elsewhere. We will also discuss high-profile examples of trolling such as “training” the Microsoft Tay chatbot, fake Antifa accounts, Russian sockpuppet accounts, and Phineas Fisher’s use of Hacking Team’s twitter account – and ask attendees to consider each as black hat attacks or grey hat attempts to point out critical societal vulnerabilities that should be “patched.” We will also talk about “troll the troll” accounts like ImposterBuster and YesYoureRacist and the role “white hat trolls” might play in auditing platforms or proposing platform-based controls. Time permitting, we will discuss art projects that trollishly critiqued the European Commission, Google AdSense, and the NSA. This will not be a lecture and it will not shy away from controversy. Join two members of the Media Manipulation Team at Data & Society to collectively consider the role trolling can play in pointing out the flaws in our attention/media landscape.

PWNING “THE TOUGHEST TARGET”: THE EXPLOIT CHAIN OF WINNING THE LARGEST BUG BOUNTY IN THE HISTORY OF ASR PROGRAM

Thursday at 11:00 in 101 Track,
Flamingo
45 minutes

Guang Gong
Alpha Team at Qihoo 360

Wenlin Yang
Alpha Team at Qihoo 360

Jianjun Dai
Security researcher of Qihoo360 Alpha Team

In recent years, Google has made many great efforts in exploit mitigation and attack surface reduction to strengthen the security of android system. It is becoming more and more difficult to remotely compromise Android phones especially Google’s Pixel phone.

The Pixel phone is protected by many layers of security. It was the only device that was not pwned in the 2017 Mobile Pwn2Own competition. But our team discovered a remote exploit chain—the first of its kind since the Android Security Rewards (ASR) program expansion, which could compromise The Pixel phone remotely. The exploit chain was reported to Android security team directly. They took it seriously and patched it quickly. Because of the severity and our detailed report, we were awarded the highest reward (\$112,500) in the history of the ASR program.

In this talk we will detail how we used the exploit chain to inject arbitrary code into system_server process and get system user permissions. The exploit chain includes two bugs, CVE-2017-5116 and CVE-2017-14904. CVE-2017-5116 is a V8 engine bug related with Webassembly and SharedArrayBuffer. It is used to get remote code execution in sandboxed Chrome render process. CVE-2017-14904 is a bug in Android’s libgralloc module that is used to escape from the sandbox. The way we used for sandbox escaping is very interesting, rarely talked about before. All details of vulnerabilities and mitigation bypassing techniques will be given in this talk.

DE-ANONYMIZING PROGRAMMERS FROM SOURCE CODE AND BINARIES

Friday at 10:00 in Track 2
45 minutes

Rachel Greenstadt
Associate Professor, Drexel University

Dr. Aylin Caliskan
Assistant professor of Computer Science, George
Washington University

Many hackers like to contribute code, binaries, and exploits under pseudonyms, but how anonymous are these contributions really? In this talk, we will discuss our work on programmer de-anonymization from the standpoint of machine learning. We will show how abstract syntax trees contain stylistic fingerprints and how these can be used to potentially identify programmers from code and binaries. We perform programmer de-anonymization using both obfuscated binaries, and real-world code found in single-author GitHub repositories and the leaked Nulled.IO hacker forum.

AUTOMATED DISCOVERY OF DESERIALIZATION GADGET CHAINS

Friday at 16:00 in 101 Track, Flamingo
45 minutes | Tool

Ian Haken
Senior Security Software Engineer, Netflix

Although vulnerabilities stemming from the deserialization of untrusted data have been understood for many years, unsafe deserialization continues to be a vulnerability class that isn’t going away. Attention on Java deserialization vulnerabilities skyrocketed in 2015 when Frohoff and Lawrence published an RCE gadget chain in the Apache Commons library and as recently as last year’s Black Hat, Muñoz and Miroshis presented a survey of dangerous JSON deserialization libraries. While much research and automated detection technology has so far focused on the discovery of vulnerable entry points (i.e. code that deserializes untrusted data), finding a “gadget chain” to actually make the vulnerability exploitable has thus far been a largely manual exercise. In this talk, I present a new technique for the automated discovery of deserialization gadget chains in Java, allowing defensive

teams to quickly identify the significance of a deserialization vulnerability and allowing penetration testers to quickly develop working exploits. At the conclusion we will also be releasing a FOSS toolkit which utilizes this methodology and has been used to successfully develop many deserialization exploits in both internal applications and open source projects.

4G: WHO IS PAYING YOUR CELLULAR PHONE BILL?

Friday at 14:00 in Track 2
45 minutes | Demo, Exploit

Dr. Silke Holtmanns
Distinguished Member of Technical Staff, Security
Expert, Nokia Bell Labs

Isha Singh
Master student, Aalto University in Helsinki (Finland)

Cellular networks are connected with each other through a worldwide private, but not unaccessible network, called IPX network. Through this network user related information is exchanged for roaming purposes or for cross-network communication. This private network has been breached by criminals and nation states. Cellular networks are extremely complex and many attacks have been already been found e.g. DoS, location tracking, SMS interception, data interception. Many attacks have been seen in practice, but not all attack are understood and not all attack avenues using the IPX network have been explored. This presentation shows how a S9 interface in 4G networks, which is used for charging related user information exchange between operators can be exploited to perform fraud attacks. A demonstration with technical details will be given and guidance on practical countermeasures.

BREAKING SMART SPEAKERS: WE ARE LISTENING TO YOU.

Sunday at 12:00 in 101 Track,
Flamingo
45 minutes | Demo, Exploit

Wu HuiYu
Security Researcher At Tencent Blade Team

Qian Wenxiang
Security Researcher At Tencent Blade Team

In the past two years, smart speakers have become the most popular IoT

device, Amazon_ Google and Apple have introduced their own smart speaker products. Most of these smart speakers have natural language recognition, chat, music playback, IoT device control, shopping, and so on. Manufacturers use artificial intelligence technology to make smart speakers have similar human capabilities in the chat conversation. However, with the smart speakers coming into more and more homes, and the function is becoming more powerful, its security has been questioned by many people. People are worried that smart speakers will be hacked to leak their privacy, and our research proves that this concern is very necessary.

In this talk, we will present how to use multiple vulnerabilities to achieve remote attack some of the most popular smart speakers. Our final attack effects include silent listening, control speaker speaking content and other demonstrations. And we’re also going to talk about how to extract firmware from BGA packages Flash chips such as EMMC, EMCP, NAND Flash, etc. In addition, it contains how to turn on debug interfaces and get root privileges by modifying firmware content and Re-soldering Flash chips, which can be of great help for subsequent vulnerability analysis and debugging. Finally, we will play several demo videos to demonstrate how we can remotely access some Smart Speaker Root permissions and use smart speakers for eavesdropping and playing voice.

EDGE SIDE INCLUDE INJECTION: ABUSING CACHING SERVERS INTO SSRF AND TRANSPARENT SESSION HIJACKING

Sunday at 13:30 in Track 3
20 minutes | Demo

ldionmarcell
Pentester at GoSecure

When caching servers and load balancers became an integral part of the Internet’s infrastructure, vendors introduced “Edge Side Includes” (ESI), a technology allowing malleability in caching systems. This legacy technology, still implemented in nearly all popular HTTP surrogates (caching/load

balancing services), is dangerous by design and brings a yet unexplored vector for web-based attacks.

The ESI language consists of a small set of instructions represented by XML tags, served by the backend application server, which are processed on the Edge servers (load balancers, reverse proxies). Due to the upstream-trusting nature of Edge servers, ESI engines are not able to distinguish between ESI instructions legitimately provided by the application server and malicious instructions injected by a malicious party. We identified that ESI can be used to perform SSRF, bypass reflected XSS filters (Chrome), and perform Javascript-less cookie theft, including HTTPOnly cookies.

Identified affected vendors include Akamai, Varnish, Squid, Fastly, WebSphere, WebLogic, F5, and countless language-specific solutions (NodeJS, Ruby, etc.). This presentation will start by introducing ESI and visiting typical infrastructures leveraging it. We will then delve into identification, exploitation of popular ESI engines, and mitigation.

DIGITAL LEVIATHAN: A COMPREHENSIVE LIST OF NATION-STATE BIG BROTHERS (FROM HUGE TO LITTLE ONES

Saturday at 14:00 in Track 2
20 minutes

Eduardo Izycki
Hacker

Rodrigo Colli
Hacker

In his notorious book Leviathan, the XVII century English philosopher Thomas Hobbes stated that: we should give our obedience to an unaccountable sovereign otherwise what awaits us is a state of nature that closely resembles civil war—a situation of universal insecurity. It looks like a lot of current political leaders have read and found the teachings of Hobbes applicable to modern day online life.

We witness the rise of the Digital Leviathan. The same apps and applications that people use to connect, express opinions and dissatisfaction

PRESENTATIONS

are used by governments (even democratic ones) to perform surveillance and censorship.

This talk will focus on evidence of Nation-State spying, performing surveillance, and censorship. The aim is to present a systematical approach of data regarding cyber attacks against political targets (NGO/political groups/media outlets/opposition), acquisition and/or use of spywares from private vendors, requested content/metadata from social media/content providers, and blocking of websites/censorship reported by multiple sources.

The findings of the research imply that:

- 25 nations that have already used cyber offensive capabilities against political targets.

- 60 nations acquired/developed spyware.

- 117 nations requested content/metadata from social media/content providers.

- 21 countries perform some level of censorship to online content.

VULNERABLE OUT OF THE BOX: AN EVALUATION OF ANDROID CARRIER DEVICES

Friday at 12:00 in Track 1
45 minutes | Audience Participation, Exploit

Ryan Johnson
Director of Research at Kryptowire

Angelos Stavrou
CEO at Kryptowire

Pre-installed apps and firmware pose a risk due to vulnerabilities that can be pre-positioned on a device, rendering the device vulnerable on purchase. This means that the vulnerabilities are present even before the user enables wireless communications and starts installing third-party apps. To quantify the exposure of the Android end-users to vulnerabilities residing within pre-installed apps and firmware, we analyzed a wide range of Android vendors and carriers using devices spanning from low-end to flagship. Our primary focus was exposing pre-positioned threats on Android devices sold by United States (US) carriers,

although our results affect devices worldwide. We will provide details of vulnerabilities in devices from all four major US carriers, as well two smaller US carriers, among others. The vulnerabilities we discovered on devices offered by the major US carriers are the following: arbitrary command execution as the system user, obtaining the modem logs and logcat logs, wiping all user data from a device (i.e., factory reset), obtaining and modifying a user's text messages, sending arbitrary text messages, and getting the phone numbers of the user's contacts, and more. All of the aforementioned capabilities are obtained outside of the normal Android permission model. Including both locked and unlocked devices, we provide details for 37 unique vulnerabilities affecting 25 Android devices with 11 of them being sold by US carriers. In this talk, we will present our framework that is capable of discovering 0-day vulnerabilities from binary firmware images and applications at scale allowing us to continuously monitor devices across different manufacturers and firmware versions. During the talk, we plan to perform a live demo of how our system works.

NSA TALKS CYBERSECURITY

Friday at 11:00 in Track 1
45 minutes

Rob Joyce
National Security Agency

The National Security Agency (NSA) has authorities for both foreign intelligence and cyber security. This unique position gives NSA insights into the ways networks are exploited and the methods that are effective in defending against threats. Over time, NSA has adapted the focus of its security efforts and continues to evolve with technologies and the adversaries we face. The talk will look back at some of the inflection points that have influenced NSA and US Government cybersecurity efforts and look at what is necessary to stay safe in the new environment.

DRAGNET: YOUR SOCIAL ENGINEERING SIDEKICK

Friday at 13:30 in Track 1
20 minutes | Demo, Tool

Truman Kain
Security Associate, Tevora

First, Dragnet collects dozens of OSINT data points on past and present social engineering targets. Then, using conversion data from previous engagements, Dragnet provides recommendations for use on your current targets: phishing templates, vishing scripts and physical pretexts- all to increase conversions with minimal effort. Finally, features like landing page cloning and domain registration (alongside your standard infrastructure deployment, call scheduling and email delivery) make Dragnet one hell of a catch.

YOUR WATCH CAN WATCH YOU! GEAR UP FOR THE BROKEN PRIVILEGE PITFALLS IN THE SAMSUNG GEAR SMARTWATCH

Sunday at 14:00 in Track 1
45 minutes | Demo, Tool, Exploit

Dongsung Kim
Graduate Student, Sungkyunkwan University

Hyoung-Kee Choi
Professor, Sungkyunkwan University

You buy a brand-new smartwatch. You receive emails and send messages, right on your wrist. How convenient, this mighty power! But great power always comes with great responsibility. Smartwatches hold precious information just like smartphones, so do they actually fulfill their responsibilities?

In this talk, we will investigate if the Samsung Gear smartwatch series properly screens unauthorized access to user information. More specifically, we will focus on a communication channel between applications and system services, and how each internal Tizen OS components play the parts in access control.

Based on the analysis, we have developed a new simple tool to discover privilege violations in Tizen-based products. We will present an analysis on the Gear smartwatch which turns out to include a number of vulnerabilities in system services.

We will disclose several previously unknown exploits in this presentation. They enable an unprivileged application to take over the wireless services, the user's email account, and more. Further discussions will center on the distribution of those exploits through a registered application in the market, and the causes of the vulnerabilities in detail.

MICRO-RENOVATOR: BRINGING PROCESSOR FIRMWARE UP TO CODE

Sunday at 13:00 in Track 2
20 minutes | Demo, Tool

Matt King
Hacker

The mitigations for Spectre highlighted a weak link in the patching process for many users: firmware (un)availability. While updated microcode was made publicly available for many processors, end-users are unable to directly consume it. Instead, platform and operating system vendors need to distribute firmware and kernel patches which include the new microcode. Inconsistent support from those vendors has left millions of users without a way to consume these critical security updates, until now. Micro-Renovator provides the ability to apply microcode updates without modifying either platform firmware or the operating system, through simple (and reversible) modifications to the EFI boot partition.

SEARCHING FOR THE LIGHT: ADVENTURES WITH OPTICSPY

Sunday at 11:00 in 101 Track, Flamingo
45 minutes | Demo

Joe Grand
Hacker

In the counter-future where we, the dissidents and hackers, have control of technology, sending secret messages through blinkenlights can let us exchange information without being detected by dystopian leaders. By modulating light in a way that the human eye cannot see, this simple, yet clever, covert channel lets us hide in plain sight. To decode such transmissions, we must employ some sort of optical receiver.

Enter OpticSpy, an open source hardware module that captures, amplifies, and converts an optical signal from a visible or infrared light source into a digital form that can be analyzed or decoded with a computer. This presentation provides a brief history of covert channels and optical communications, explores the development process and operational details of OpticSpy, and gives a variety of demonstrations of the unit in action.

DESIGNING AND APPLYING EXTENSIBLE RF FUZZING TOOLS TO EXPOSE PHY LAYER VULNERABILITIES

Sunday at 12:00 in Track 3
45 minutes | Demo, Tool, Exploit

Matt Knight
Senior Security Engineer, Cruise Automation

Ryan Speers
Director of Research, Ionic Security

In this session, we introduce an open source hardware and software framework for fuzzing arbitrary RF protocols, all the way down to the PHY. While fuzzing has long been relied on by security researchers to identify software bugs, applying fuzzing methodologies to RF and hardware systems has historically been challenging due to siloed tools and the limited capabilities of commodity RF chipsets.

We created the TumbleRF fuzzing orchestration framework to address these shortfalls by defining core fuzzing logic while abstracting a hardware interface API that can be mapped for compatibility with any RF driver. Thus, supporting a new radio involves merely extending an API, rather than writing a protocol-specific fuzzer from scratch.

Additionally, we introduce Orthrus, a low-cost 2.4 GHz offensive radio tool that provides PHY-layer mutability to offer Software Defined Radio-like features in a flexible and low-latency embedded form factor. By combining the two, researchers will be able to fuzz and test RF protocols with greater depth and precision than ever before.

Attendees can expect to leave this talk with an understanding of how RF

and hardware physical layers actually work, and how to identify security issues that lie latent in these designs.

THROUGH THE EYES OF THE ATTACKER: DESIGNING EMBEDDED SYSTEMS EXPLOITS FOR INDUSTRIAL CONTROL SYSTEMS

Saturday at 10:00 in 101 Track, Flamingo
45 minutes | Demo

Marina Krotofil
Principal Analyst, FireEye

Ali Abbasi
Postdoctoral researcher, Ruhr University Bochum

Thorsten Holz
Professor, Ruhr University Bochum

In 2017, FireEye conducted an incident response at a critical infrastructure facility where a sophisticated threat actor deployed the TRITON attack framework for implanting Safety Instrumented System (SIS) controllers with a passive backdoor, which would allow an attacker to inject potentially destructive payloads at a later point in time. TRITON is the most complex publicly known embedded system exploit to date. While the functionality of the malware is understood, little known about attacker efforts when developing such an implant. With a timeline of exploit development like TRITON being in a year range, complex embedded exploitation is currently considered to be a boutique hacking. However, the public release of much of the TRITON code can now facilitate less experienced threat actors with designing similar exploits. The goal of this talk is to provide the audience with a "through the eyes of the attacker" experience when designing advanced embedded systems exploits for Industrial Control Systems (ICS). This talk is based on our extensive experience in reverse engineering Real Time Operating Systems (RTOS)/firmwares and developing embedded exploits to cause physical damage.

In the first part of the talk we will explain how to convert an 'undocumented device' into malicious code. We will share how to purchase industrial equipment and obtain needed documentation.

PRESENTATIONS

After obtaining control over an embedded system, an actual attack still need to be performed. In the second part of the talk will concentrate on discovering exploitable firmware and hardware design features which would allow an attacker to impact industrial controller functions. We will present several scenarios such as hijacking internal clock, suppressing interrupts (IRQ config attack) and manipulation of the interrupt vector table (IVT), CPU pin configuration attack and placing code into TCM cache so it would not be even visible in the memory.

The TRITON payload can be thought of as a four-stage shellcode. Attack code related to first three stages constituted a discussed backdoor implant capable of receiving and executing the fourth stage. This stage would have been an actual 'physical damage payload' performing the disruptive operations. However, the attacker was discovered while preparing the implant, before advancing to physical damage stage. In this part of the talk we will show how one can symbolically execute TRITON using ANGR framework and test a code for damage scenario written for any CPU/hardware architecture of choice.

Developing embedded exploits requires a significant amount of effort but it is totally worth of investment. While a small fraction of asset owners is slowly embracing ICS network monitoring solutions, the attackers are going one layer lower—into the control equipment (race-to-the-bottom). Developing embedded implants is worth the efforts due to lacking tools for detecting such implants and we will see more of advanced embedded exploitation in the nearest future.

THE LOPHT TESTIMONY, 20 YEARS LATER (AND OTHER THINGS YOU WERE AFRAID TO ASK)

Friday at 17:00 in Track 2
45 minutes | Audience Participation

LOpht Heavy Industries
Hacker Collective

Elinor Mills
Senior Vice President of Content and Media Strategy at
Bateman Group

DilDog
Hacker, Co-Founder, Veracode

Joe Grand, Kingpin
Hacker

Space Rogue
Global Strategy Lead for X-Force Red, IBM

Mudge
Head of Security, Stripe.

Silicosis
Hacker

John Tan
Hacker

Weld Pond
Hacker, Co-Founder, Veracode

2018 is the 20th anniversary of the hacker think-tank L0pht Heavy Industries testimony before the US Senate Homeland Security & Governmental Affairs Committee on the topic of weak computer security in government. The testimony made national news when the group announced they could take down the Internet in 30 minutes. It was also the first-time hackers using handles appeared before a US Legislative body.

Members of the L0pht have grown from their hacker roots to become distinguished leaders and contributors in the security community and beyond. They run multi-million dollar security-focused organizations, have lobbied the government for better security laws, work for some of the largest companies in the world, and continue to spread the message of the positive aspects of hacking.

With several of the L0pht's original members, this discussion will cover the original testimony and the changes that have happened over the last 20 years. Is the government any more secure? Have they provided enough influence to help protect its citizens' data? What steps should we take to ensure user security and privacy in the future? We are hoping for audience participation and also welcome questions about any other time in the L0pht's relatively short, but poignant, existence.

WHO CONTROLS THE CONTROLLERS: HACKING CRESTRON IOT AUTOMATION SYSTEMS

Friday at 12:00 in Track 3
45 minutes | Demo, Exploit

Ricky "HeadlessZeke" Lawshae
Security Researcher, Trend Micro

While you may not always be aware of them or even have heard of them, Crestron devices are everywhere. They can be found in universities, modern office buildings, sports arenas, and even high-end Las Vegas hotel rooms. If an environment has a lot of audio/video infrastructure, needs to interconnect or automate different IoT and building systems, or just wants the shades to close when the TV is turned on, chances are high that a Crestron device is controlling things from behind the scenes. And as these types of environments become the norm and grow ever more complex, the number of systems that Crestron devices are connected to grows as well. But it is in large part because of this complexity that installing and programming these devices is difficult enough without considering adding security. Instead of being a necessity, it's an extra headache that almost always gets entirely passed over. In this talk, I will take a look at different Crestron devices from a security perspective and discuss the many vulnerabilities and opportunities for fun to be found within. I will demonstrate both documented and undocumented features that can be used to achieve full system compromise and show the need to make securing these systems a priority, instead of an afterthought, in every deployment. In short, hijinx will ensue.

I'LL SEE YOUR MISSILE AND RAISE YOU A MIRV: AN OVERVIEW OF THE GENESIS SCRIPTING ENGINE

Friday at 17:00 in Track 1
45 minutes | Demo, Audience Participation, Tool

Alex Levinson
Senior Security Engineer

Dan Borges
Hacker

Vyrus
Hacker

Typically, the activities of a malware attack occur on an execution timeline that generally consists of 3 segments—the vector, the stage, and the persistence. First, a vector, or method of exploitation is identified. This could be anything from logging in over a credentialed method like RDP or SSH and running a malicious payload directly, to exploiting a memory corruption vulnerability remotely. Second, that access is leveraged into running malicious code that prepares the victim for the deployment of persistence (commonly "implant"). While segments one and three have been extensively automated, a effective automated utility for deploying persistence in a dynamic and unified context has yet to present itself.

Enter the Genesis Scripting Engine.

The Genesis Scripting Engine, or Gscript for short, is a framework for building multi-tenant executors for several implants in a stager. The engine works by embedding runtime logic (powered by the V8 Javascript Virtual Machine) for each persistence technique. This logic gets run at deploy time on the victim machine, in parallel for every implant contained with the stager. The Gscript engine leverages the multi-platform support of Golang to produce final stage one binaries for Windows, Mac, and Linux.

This talk will consist of an overview of the origins of the project, a technical deep dive into the inner workings including the modified Javascript VM, a walk through of the CLI utility, and examples of how we've leveraged Gscript in the real world.

Multiple demos involving practical application scenarios will be presented, as well as an opportunity for audience members to submit their own implants and have them built into a hydra on stage in a matter of minutes.

BOOBY TRAPPING BOXES

Saturday at 15:00 in Track 3
45 minutes | Demo, Tool

Ladar Levison
Founder, Lavabit LLC

hon1nbo
Proprietor, Hacking & Coffee LLC

Ever worry about the hardware you leave behind? In a world where servers are co-located, and notebooks get left in hotel rooms, the ability to resist tampering, and if necessary actively respond to attack, has become increasingly important. And of course everybody knows the best booby traps are the ones you don't know are there. This talk will prepare you for life in 1984, where the maids are evil, and step brothers can't be trusted. Whether your running servers as a high value target, or simply want to protect your Monero private key, this talk will show you to achieve FIPS 140-2 level 4 security, without the FIPS 140-2 level 4 price tag. Specifically, we'll cover acquisition considerations, physical hardening, firmware mitigation, tamper detection and more.

PLEASE DO NOT DUPLICATE: ATTACKING THE KNOX BOX AND OTHER KEYED ALIKE SYSTEMS

Friday at 10:30 in Track 3
20 minutes | Demo, Tool

m0l0ch_
Hacker

Knox Boxes, along with other rapid entry systems are increasing in popularity, as they allow first responders such as police, fire, and paramedics to quickly gain access to a building in the event of an emergency without having to force entry. These devices rely on the security and key control provided by various locks to prevent unauthorized access to buildings. In this talk, I will focus on vulnerabilities of the widely used Knox Box and Medeco cam lock to key duplication attacks. I will demonstrate how a sufficiently skilled attacker could obtain a key that would grant them access to thousands of residential and commercial buildings throughout America, as well as show off new tools designed to streamline the process of duplicating physical keys using CAD and 3D printing. What could possibly go wrong when someone tries to backdoor an entire city?

PLAYING MALWARE INJECTION WITH EXPLOIT THOUGHTS

Saturday at 14:00 in Track 3
20 minutes | Demo, Tool, Exploit

Sheng-Hao Ma
CSIE, NTUST

In the past, when hackers did malicious program code injection, they used to adopt RunPE, AtomBombing, cross-process creation threads, and other approaches. They could forge their own execution program as any critical system service. However with increasing process of anti-virus techniques, these sensitive approaches have been gradually proactively killed. Therefore, hackers began to aim at another place, namely memory-level weakness, due to the breakages of critical system service itself.

This agenda will simply introduce a new memory injection technique that emerged after 2013, PowerLoadEx. Based on this concept, three new injection methods will be disclosed as well. These makes good use of the memory vulnerability in Windows to inject malicious behavior into system critical services. The content will cover Windows reverse analysis, memory weakness analysis, how to use and utilize, and so on. The relevant PoC will be released at the end of the agenda.

MAN-IN-THE-DISK

Sunday at 13:00 in Track 1
20 minutes | Demo, Tool, Exploit

Slava Makraveev
Security Researcher, Check Point

Most of modern OS are using sandboxing in order to prevent malicious apps from affecting other apps or even harming the OS itself. Google is constantly reinforcing Android's sandbox protection, introducing new features to prevent any kind of sandbox bypass.

In this talk we want to shed new light on a less known attack surface which affects all Android devices and allows an attacker to hijack the communication between privileged apps and the disk, bypassing Android's latest sandbox protection.

The problem begins when privileged apps interact with files

PRESENTATIONS

stored in exposed areas, and even worse, some of them will unintentionally break the sandbox by insecurely appending such data to its confinements.

Can you imagine if someone could execute code in the context of your keyboard, or install an unwanted app without your consent? Well... It's hardly within the realm of imagination.

The external storage and network based vulnerabilities we discovered, can be leveraged by the attacker to corrupt data, steal sensitive information or even take control of your device.

SECURING OUR NATION'S ELECTION INFRASTRUCTURE

Friday at 10:00 in Track 3
20 minutes

Jeanette Manfra
Assistant Secretary, Office of Cybersecurity and Communications, Department of Homeland Security

Fair elections are at the core of every democracy and are of paramount importance to our national security. The confidence in our electoral process is fundamental to ensuring that every vote- and therefore every voice- matters. In recent years, our Nation has become increasingly uneasy about the potential threats to our election infrastructure. The activities to undermine the confidence in the 2016 presidential election have been well documented and the United States (U.S.) Government has assessed that our adversaries will apply lessons learned from the 2016 election and will continue in their attempts to influence the U.S. and their allies' upcoming elections, including the 2018 mid-term elections. As the lead agency for securing the Nation's cyber infrastructure, the Department of Homeland Security (DHS) has a mission to maintain public trust and protect America's election systems. In January 2017, the DHS Secretary designated election systems as critical infrastructure. This designation means election infrastructure has become a priority in shaping our planning and policy initiatives, as well as how we allocate our resources. DHS is working directly with election officials across 8,000 election jurisdictions and throughout

55 States and territories, to help them safeguard their systems. As the threat environment evolves, DHS will continue to work with state and local partners to enhance our understanding of the threat, share timely and actionable threat information, and provide essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency. DHS is committed to ensuring that our adversaries never succeed with their campaign to undermine our democracy.

LOOKING FOR THE PERFECT SIGNATURE: AN AUTOMATIC YARA RULES GENERATION ALGORITHM IN THE AI-ERA

Saturday at 13:00 in Track 3
20 minutes | Demo, Tool

Andrea Marcelli
PhD Student and Security Researcher. Politecnico di Torino

Given the high pace at which new malware variants are generated, antivirus programs struggle to keep their signatures up-to-date, and AV scanners suffer from a considerable quantity of false negatives. The generation of effective signatures against new malware variants, while avoiding false positive detections, is a highly desirable but challenging task, typically requiring a substantial portion of human expert's time. Artificial intelligence techniques can be applied to solve the malware signature generation problem.

The ultimate goal is to develop an algorithm able to automatically create a generalized family signature, eventually reducing threat exposure and increasing the quality of the detection. The proposed technique automatically generates an optimal signature to identify a malware family with very high precision and good recall using heuristics, evolutionary and linear programming algorithms.

In this talk I will present YaYaGen (Yet Another YARA Rule Generator), a tool to automatically generate Android malware signatures. Performances have been evaluated on a massive dataset of millions of applications available in the Koodous project, showing that in a few minutes the

algorithm can generate precise ruleset able to catch 0-day malware, better than human generated ones.

ONE-CLICK TO OWA

Friday at 13:00 in Track 3
20 minutes | Demo, Tool

William Martin
Security & Privacy Senior Associate

With the presence of 2FA/MFA solutions growing, the attack surface for external attackers that have successfully phished/captured/cracked credentials is shrinking. However, many 2FA/MFA solutions leave gaps in their coverage which can allow attackers to leverage those credentials. For example, while OWA may be protected with 2FA, the Exchange Web Services Management API (EWS) offers many of the same features and functionalities without the same protections.

In this talk, I will introduce ExchangeRelayX, an NTLM relay tool that provides attackers with access to an interface that resembles a victim's OWA UI and has many of its functionalities - without ever cracking the relayed credentials. ExchangeRelayX takes advantage of the gap in some 2FA/MFA solutions protecting Exchange, potentially resulting in a single-click phishing scheme enabling an attacker to exfiltrate sensitive data, perform limited active-directory enumeration, and execute further internal phishing attacks.

SMBETRAY: BACKDOORING AND BREAKING SIGNATURES

Saturday at 14:00 in Track 1
45 minutes | Demo, Tool

William Martin
Security & Privacy Senior Associate

When it comes to taking advantage of SMB connections, most tools available to penetration testers aim for system enumeration or for performing relay attacks to gain RCE. If signatures are required, or if the victims relayed are not local admins anywhere, that can put a real stint in leveraging SMB to gain any serious footholds in a network. Fortunately, the mentioned attacks are only the tip of the iceberg of the ways to gain

RCE with insecure SMB connections – and there's a new tool to help take full advantage of these opportunities.

YOU'RE JUST COMPLAINING BECAUSE YOU'RE GUILTY: A DEF CON GUIDE TO ADVERSARIAL TESTING OF SOFTWARE USED IN THE CRIMINAL JUSTICE SYSTEM

Saturday at 10:00 in Track 2
45 minutes | Demo

Dr. Jeanna N. Matthews:
Associate Professor, Clarkson University and Fellow, Data and Society

Nathan Adams
Systems Engineer, Forensic Bioinformatic Services

Jerome Greco
Digital Forensics Staff Attorney, Legal Aid Society

Software is increasingly used to make huge decisions about people's lives and often these decisions are made with little transparency or accountability to individuals. If there is any place where transparency, third-party review, adversarial testing and true accountability is essential, it is the criminal justice system. Nevertheless, proprietary software is used throughout the system, and the trade secrets of software vendors are regularly deemed more important than the rights of the accused to understand and challenge decisions made by these complex systems. In this talk, we will lay out the map of software in this space from DNA testing to facial recognition to estimating the likelihood that someone will commit a future crime. We will detail the substantial hurdles that prevent oversight and stunning examples of real problems found when hard won third-party review is finally achieved. Finally, we will outline what you as a concerned citizen/hacker can do. Nathan Adams will demo his findings from reviewing NYC's FST source code, which was finally made public by a federal judge after years of the city's lab fighting disclosure or even review. Jerome Greco will provide his insight into the wider world of software used in the criminal justice system—from technology that law enforcement admits to using but expects the public to trust without question to technology that

law enforcement denies when the evidence says otherwise. Jeanna Matthews will talk about the wider space of algorithmic accountability and transparency and why even open source software is not enough.

SEX WORK AFTER SESTA/FOSTA

Saturday at 14:30 in Track 2
20 minutes

Maggie Mayhem
MaggieMayhem.Com

Surveillance had been a fact of life for sex workers wherever they have faced prohibition. Only two elements, communication and association, can differentiate between commercial and personal sex, criminal enforcement of prostitution laws have necessarily meant targeting the speech and affiliation of perceived sex workers. Enforcement of this nature is facilitated by profiling, institutional bias, and broad overreaching policies that fundamentally violate individual human rights. This has included condoms as evidence, non-consensual medical screenings, and targeted harassment of black transgender women as well as license plate recording projects and stings that focus disrupting immigration or migrant workers.

For all of its risks, screening potential clients is safer over email than it is in person during a street based negotiation often in an isolated part of town. SESTA (Stop Enabling Sex Traffickers Act) comes at a time when compelling research demonstrates that Craigslist resulted in a 17% drop in the female homicide rate. SESTA will also put victims at risk by delaying their identification and recovery by eliminating a digital paper trail. Additionally, Section 230 of the Communications Decency Act is a vital protection for a free internet. Subverting SESTA will create greater economic disparity between sex workers and ultimately empower pimps and agencies over independent providers.

AN ATTACKER LOOKS AT DOCKER: APPROACHING MULTI-CONTAINER APPLICATIONS

Friday at 11:00 in 101 Track, Flamingo
45 minutes | Demo

Wesley McGrew
Director of Cyber Operations, HORNE Cyber

Containerization, such as that provided by Docker, is becoming very popular among developers of large-scale applications. The good news: this is likely to make your life easier as an attacker.

While exploitation and manipulation of traditional monolithic applications might require specialized experience and training in the target languages and execution environment, applications made up of services distributed among multiple containers can be effectively explored and exploited "from within" using many of the system- and network-level techniques that attackers, such as penetration testers, already know.

The goal of this talk is to provide a hacker experienced in exploitation and post-exploitation of networks and systems with an exposure to containerization and the implications it has on offensive operations. Docker is used as a concrete example for the case study. A hacker can expect to leave this presentation with a practical exposure to multi-container application post-exploitation.

80 TO 0 IN UNDER 5 SECONDS: FALSIFYING A MEDICAL PATIENT'S VITALS

Saturday at 16:00 in Track 1
45 minutes | Demo

Douglas McKee
Senior Security Researcher for the McAfee Advanced Threat Research team

It seems each day that passes brings new technology and an increasing dependence upon it. The medical field is no exception; medical professionals rely upon technology to provide them with accurate information and base life-changing decisions on this data.

In recent years there has been more attention paid to the security of medical devices; however, there has been little research done on the unique protocols used by these devices. In large, health care systems

PRESENTATIONS

medical personnel take advantage of to make decisions on patient treatment and other critical care, use central monitoring stations. This information is gathered from many devices on the network using uncommon networking protocols. What if this information wasn't accurate when a doctor prescribed medication? What if a patient was thought to be peacefully resting, when in fact they are under cardiac arrest?

McAfee's Advanced Threat Research team has discovered a weakness in the RWHAT protocol, one of the networking protocols used by medical devices to monitor a patient's condition. This protocol is utilized in some of the most critical systems used in hospitals. This weakness allows the data to be modified by an attacker in real-time to provide false information to medical personnel. Lack of authentication also allows rogue devices to be placed onto the network and mimic patient monitors.

This presentation will include a technical dissection of the security issues inherent in this relatively unknown protocol. It will describe real-world attack scenarios and demonstrate the ability to modify the communications in-transit to directly influence the receiving devices. We will also explore the general lack of security mitigations in the medical devices field, the risks they pose, and techniques to address them. The talk will conclude with a demonstration using actual medical device hardware and a live modification of a patient's critical data.

EXPLOITING ACTIVE DIRECTORY ADMINISTRATOR INSECURITIES

Saturday at 11:00 in Track 1
45 minutes | [Demo](#)

Sean Metcalf
CTO, Trimarc

Defenders have been slowly adapting to the new reality: Any organization is a target. They bought boxes that blink and software that floods the SOC with alerts. None of this matters as much as how administration is performed: Pop an admin, own the system. Admins are being dragged into a new paradigm where they

have to more securely administer the environment. What does this mean for the pentester or Red Teamer?

Admins are gradually using better methods like two-factor and more secure administrative channels. Security is improving at many organizations, often quite rapidly. If we can quickly identify the way that administration is being performed, we can better highlight the flaws in the admin process.

This talk explores some common methods Active Directory administrators (and others) use to protect their admin credentials and the flaws with these approaches. New recon methods will be provided on how to identify if the org uses an AD Red Forest (aka Admin Forest) and what that means for one hired to test the organization's defenses, as well as how to successfully avoid the Red Forest and still be successful on an engagement.

Some of the areas explored in this talk:

- Current methods organizations use to administer Active Directory and the weaknesses around them.
- Using RODCs in the environment in ways the organization didn't plan for (including persistence).
- Exploiting access to agents typically installed on Domain Controllers and other highly privileged systems to run/install code when that's not their typical purpose.
- Discovering and exploiting an AD forest that leverages an AD Admin Forest (aka Red Forest) without touching the Admin Forest. If you are wondering how to pentest/red team against organizations that are improving their defenses, this talk is for you. If you are a blue team looking for inspiration on effective defenses, this talk is also for you to gain better insight into how you can be attacked.

RIDEALONG ADVENTURES: CRITICAL ISSUES WITH POLICE BODY CAMERAS

Saturday at 12:00 in Track 3
45 minutes | [Demo](#), [Tool](#), [Exploit](#)

Josh Mitchell
Principal cybersecurity Consultant, Nuix

The police body camera market has been growing in popularity over the last few years. A recent (2016) Johns Hopkins University market survey found 60 different models have been produced specifically for law enforcement use. Rapid adoption is fueling this meteoric increase in availability and utilization. Additionally, device manufactures are attempting to package more and more technology into these devices. This has caused a deficiency in local municipalities' skills and budget to accurately assess the attack surface and exposure to the organization. Furthermore, departmental policies and procedures governing the secure deployment of these devices is largely insufficient.

At DEF CON, we will be introducing tactics, techniques, and procedures to assess the security of these devices. We will cover attacks against the physical devices, RF components, smartphone app's, and desktop software. The capabilities demonstrated and discussed will encompass publicly and privately available technologies. Additionally, the talk will cover multiple products and vendors, shedding light on industry wide issues and trends. Finally, we will be releasing software to detect and track various devices and tie these issues into real world events.

COMPRESSION ORACLE ATTACKS ON VPN NETWORKS

Saturday at 11:00 in Track 2
45 minutes | [Demo](#), [Tool](#)

Nafeez
Security Researcher

Security researchers have done a good amount of practical attacks in the past using chosen plain-text attacks on compressed traffic to steal sensitive data. In spite of how popular CRIME and BREACH were, little was talked about how this class of attacks was relevant to VPN networks. Compression oracle attacks are not limited to just TLS protected data. In this talk, we try these attacks on browser requests and responses which usually tunnel their HTTP traffic through VPNs. We also show a case study with a well-known VPN server and their plethora of clients. We then

go into practical defenses and how mitigations in HTTP/2's HPACK and other mitigation techniques are the way forward rather than claiming 'Thou shall not compress traffic at all.' One of the things that we would like to showcase is how impedance mismatches in these different layers of technologies affect security and how they don't play well together.

ONE STEP AHEAD OF CHEATERS: INSTRUMENTING ANDROID EMULATORS

Saturday at 13:00 in 101 Track, Flamingo
20 minutes | [Demo](#), [Tool](#)

Nevermoe (@n3v3rm03)
Security Engineer, DeNA Co., Ltd.

Commercial Android emulators such as NOX, BlueStacks and Leidian are very popular at the moment and most games can run on these emulators fast and soundly. The bad news for game vendors is that these emulators are usually shipped with root permission in the first place. On the other hand, cheating tools developers are happy because they can easily distribute their tools to abusers without requiring the abusers to have a physical rooted device, nor do they need to perform laborious tuning for different Android OS / firmware version. However, luckily for game vendors, commercial Android emulators usually use an x86/ARM mixed-mode emulation for speed-up. As a result, a standard native hooking/DBI framework won't work on this kind of platform. This drawback could discourage the cheating developers.

In this talk, I will introduce a native hooking framework on such a kind of mixed-mode emulators. The talk will include the process start routine of both command-line applications and Android JNI applications as well as how these routines differ on an emulator. The different emulation strategies adopted by different emulators and runtime environments (Dalvik/ART) will also be discussed. Based on these knowledge, I will explain why the existing hooking/DBI frameworks do not work on these emulators and how to make one that works.

Lastly, I will present a demo of using this hooking framework to cheat a game on emulator. With this demo, I will discuss how the dark market of mobile game cheating may develop in the foreseeable future.

REVERSE ENGINEERING, HACKING DOCUMENTARY SERIES

Friday at 17:00 in Track 3
45 minutes | [Demo](#)

Michael Lee Nirenberg
Director, Restraining Order, Ltd

Dave Buchwald
Producer

We will present a sample scene and panel talk on our documentary series Reverse Engineering to the hacking community, which has been in the works for 4 years. We have dozens of interviews spanning the first 3 decades of computer hacking, ultimately there will be hundreds. It's a big story, but for the purposes of DEF CON, we've put together a 17 min. Scene covering the 80s WarGames/Legion of Doom-era of computer hacking in the US.

We've spoken to great people, but there are other viewpoints—this is a history that needs to be told by 1st person accounts. The accuracy and strength of our completed series is tantamount to the quality of who we interview and the questions that get asked. Accuracy is particularly important, there's been no shortage of media hype and lies regarding hacking since the 1980s.

Our vision for this film series is inclusive and collaborative. We'd like to hear from attendees how to best tell the origin story of hacking to new generations, and more so the outside world who've been fed a lot of myths by the media. Those are the lawmakers and citizens of tomorrow that we need to reach. Little attention has been paid to the pioneering hacker spirit that has literally changed every aspect of life. We want to address and correct that.

EFF FIRESIDE HAX (AKA ASK THE EFF)

Saturday at 20:00-22:00 in Roman Chillout
[Fireside Hax](#) | [Audience Participation](#)

Kurt Opsahl
Deputy Executive Director & General Counsel, Electronic Frontier Foundation

Nate Cardozo
EFF Senior Staff Attorney

Jamie Lee Williams
EFF Staff Attorney

Andrés Arrieta
Technology Products Manager

Katiza Rodriguez
International Rights Director

Nathan 'nash' Sheard
Grassroots Advocacy Organizer

Relax and enjoy a Fireside Hax chat while you get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This Fireside Hax discussion will include updates on current EFF issues such as the government's effort to undermine encryption (and add backdoors), the fight for network neutrality, discussion of our technology projects to spread encryption across the Web and emails, updates on cases and legislation affecting security research, and much more. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.

REVOLTING RADIOS

Friday at 14:00 in Track 3
45 minutes | [Demo](#), [Tool](#)

Michael Ossmann
Great Scott Gadgets

Dominic Spill
Great Scott Gadgets

There are many Software Defined Radios (SDRs) available, with a great deal of time and effort having gone in to their design. These are not those radios. We present four radios that we have designed using crude, novel, and sometimes ridiculous methods for transmitting and receiving signals.

The arrival of SDR allowed more hackers than ever to experiment with radio protocols, but we're

PRESENTATIONS

still using hardware built by other people. In the time honored hacker tradition of rolling our own tools, we'll demonstrate four simple radios that can be home-built using commonly available parts for little to no cost.

IT WISN'T ME, ATTACKING INDUSTRIAL WIRELESS MESH NETWORKS

Saturday at 10:00 in Track 1
45 minutes | Demo

Erwin Paternotte
Lead security consultant at Nixu

Mattijs van Ommeren
Principal security consultant at Nixu

Wireless sensor networks are commonly thought of as IoT devices communicating using familiar short-range wireless protocols like Zigbee, MiWi, Thread and OpenWSN. A lesser known fact is that about a decade ago, two industrial wireless protocols (WirelessHART and ISA100.11a) have been designed for industrial applications, which are based on the common IEEE 802.15.4 RF standard. These Wireless Industrial Sensor Networks (WISN) are used in process field device networks to monitor temperature, pressure, levels, flow or vibrations. The petrochemical industry uses WISN in oil and gas fields and plants around the world.

Both IEC ratified standards have been commonly praised by the ICS industry for their security features, including strong encryption on multiple layers within the protocol stack, resistance to RF interference, and replay protection. While the standards in general look safe on paper, there are potential interesting attack vectors that require verification. However, security research so far has not yielded any significant results beyond basic attack vectors. Often these attacks have only been theorized, and not (publicly) demonstrated. In addition, vendor implementations have not been thoroughly tested for security by independent third parties, due to protocol complexity and the lack of proper (hardware/software) tools. We strongly believe in Wright's principle, "Security does not improve until practical tools for exploration of the attack surface are made available."

THINSIM-BASED ATTACKS ON MOBILE MONEY SYSTEMS

Thursday at 10:00 in 101 Track, Flamingo
45 minutes | Demo, Exploit

Rowan Phipps
Undergraduate researcher, University of Washington

Phone-based mobile money is becoming the dominant paradigm for financial services in the developing world processing more than a billion dollars per day for over 690 million users. For example, mPesa has an annual cash flow of over thirty billion USD, equivalent to nearly half of Kenya's GDP. Numerous other products exist inside of nearly every other market, including GCash in the Philippines and easyPaisa in Pakistan. As a part of this growth, competitors have appeared who leverage ThinSIMs, small SIM card add ons, to provide alternative mobile money implementations without operating their own mobile networks. However, the security implications of ThinSIMs are not well understood.

This talk dives into decade old telecom standards to explore how ThinSIMs work and what attackers of mobile money systems can do when they control the interface between the SIM card and the phone. We will also demo two proof of concept exploits that use ThinSIMs to steal money from mobile money platforms and detail the difficulties of defense.

OH NOES!: A ROLE PLAYING INCIDENT RESPONSE GAME

Friday at 20:00-22:00 in Roman Chillout
Fireside Hax | Demo, Audience Participation, Tool

Bruce Potter
Founder, The Shmoo Group

Robert Potter
Hacker

The term "incident response exercise" can strike fear in the hearts of even the mostly steely-eyed professional. The idea of sitting around a table, talking through a catastrophic security event can be both simultaneously exhausting and incredibly boring. However, what instead of an participating in

an "incident response exercise," you instead got to plan an "incident response role playing game?"

Enter our IR roleplaying game, "Oh Noes! An Adventure Through the Cybers and Shit." As part of our day job, we do quarterly IR exercises. In order to make these exercises more engaging, more fun, and more useful, we turned these exercises into a role playing game. We found it so useful and fun, we're releasing it at DEF CON along with numerous scenarios for your dungeon master to take you through.

At this talk, we will talk about gamifying IR exercises and the rules of Oh Noes! We will equip you with dice and your own character sheet and we will walk you through the character creating process. That's right, in Oh Noes! you create your own character with specific skills and abilities that you level up as you play. A group of us will play through a short scenario so you can see how the game works. We will provide several sample scenarios, some ripped from the headlines (and some cribbed from @badthingsdaily) as well as provide guidance on what makes successful scenarios as you transition to be your own dungeon master.

ALL YOUR FAMILY SECRETS BELONG TO US: WORRISOME SECURITY ISSUES IN TRACKER APPS

Saturday at 16:00 in Track 2
45 minutes | Demo, Exploit

Dr. Siegfried Rasthofer
Fraunhofer SIT

Stephan Huber
Hacker

Dr. Steven Arzt
Hacker

Google Play Store provides thousands of applications for monitoring your children/family members. Since these apps deal with highly sensitive information, they immediately raise questions on privacy and security. Who else can track the users? Is this data properly protected? To answer these questions, we analyzed a selection of the most popular tracking apps from the Google Play Store.

Many apps and services suffer from grave security issues. Some apps

use self-made algorithms instead of proper cryptography for data storage and transmission. Others do not even attempt to protect their communication at all and make use of the unprotected http protocol, or even give an attacker full access to a vulnerable backend system. Hard coded database credentials in apps allowed access to all stored user locations. We would be able to extract hundreds of thousands of tracking profiles, even in real time. In others, this wasn't even necessary, because the user authentication could be bypassed altogether. Flaws in server API allowed us to extract all user credentials (1.7m plain text passwords), further we saw full communication histories containing messages, pictures and location data.

In total, the state of tracker apps is worrisome, effectively leading to users unknowingly installing espionage software on their devices.

TINEOLA: TAKING A BITE OUT OF ENTERPRISE BLOCKCHAIN

Saturday at 12:00 in Track 1
45 minutes | Demo, Tool

Stark Riedesel
Synopsis, Senior Consultant

Parsia Hakimian
Synopsis, Senior Consultant

Blockchain adaptation has reached a fever pitch, and the community is late to the game of securing these platforms against attack. With the open source community enamored with the success of Ethereum, the enterprise community has been quietly building the next generation of distributed trustless applications on permissioned blockchain technologies. As of early 2018, an estimated half of these blockchain projects relied on the Hyperledger Fabric platform.

In this talk we will discuss tools and techniques attackers can use to target Fabric. To this end we are demoing and releasing a new attack suite, Tineola, capable of performing network reconnaissance of a Hyperledger deployment, adding evil network peers to this deployment, using existing trusted peers for lateral network movement with reverse shells, and fuzzing application code deployed on Fabric.

As George Orwell said: "Who controls the past controls the future. Who controls the present controls the past." This talk will demonstrate how a sufficiently armed red team can modify the blockchain past to control our digital future.

BREAKING EXTREME NETWORKS WINGOS: HOW TO OWN MILLIONS OF DEVICES RUNNING ON AIRCRAFTS, GOVERNMENT, SMART CITIES AND MORE.

Sunday at 11:00 in Track 1
45 minutes | Demo, Exploit

Josep Pi Rodriguez
Senior security consultant, IOActive

Extreme network's embedded WingOS (Originally created by Motorola) is an operating system used in several wireless devices such as access points and controllers. This OS is being used in Motorola devices, Zebra devices and Extreme network's devices. This research started focusing in an access point widely used in many Aircrafts by several worldwide airlines but ended up in something bigger in terms of devices affected as this embedded operating system is not only used in AP's for Aircrafts but also in Healthcare, Government, Transportation, Smart cities, small to big enterprises... and more.

Based on public information, we will see how vulnerable devices are actively used (outdoors) in big cities around the world. But also in Universities, Hotels, Casinos, Big companies, Mines, Hospitals and provides the Wi-Fi access for places such as the New York City Subway.

In this presentation we will show with technical details how several critical vulnerabilities were found in this embedded OS. First we will introduce some internals and details about the OS and then we will show the techniques used to reverse engineering the mipsN32 ABI code for the Cavium Octeon processor. It will be discussed how some code was emulated to detect how a dynamic password is generated with a cryptographic algorithm for a root shell backdoor. Besides, it will be shown how

some protocols used by some services were reverse engineered to find unauthenticated heap and stack overflow vulnerabilities that could be exploitable through Wireless or Ethernet connection.

This OS also uses a proprietary layer 2/3 protocol called MiNT. This protocol is used for communication between WingOS devices through VLAN or IP. This protocol was also reverse engineered and remote heap/stack overflow vulnerabilities were found on services using this protocol and will be shown. As a live demonstration, 2 devices will be used to exploit a remote stack overflow chaining several vulnerabilities as the attacker could do inside an aircraft (or other scenarios) through the Wi-Fi. As there are not public shellcodes for mipsN32 ABI, the particularities of creating a Shellcode for mipsN32 ABI will be also discussed.

REAPING AND BREAKING KEYS AT SCALE: WHEN CRYPTO MEETS BIG DATA

Saturday at 13:00 in Track 2
20 minutes | Demo, Audience Participation, Tool

Yolan Romailier
Security Researcher at Kudelski Security

Nils Amiet
Security Engineer at Kudelski Security

Public keys are everywhere, after all, they are public. These keys are waiting to be reaped by those who know their real value. Hidden behind this public face lurks some potentially dangerous issues which could lead to a compromise of data and privacy.

Leveraging hundreds of minion devices, we built a public key reaping machine (which we are open sourcing) and operated it on a global scale. Collected keys are tested for vulnerabilities such as the recent ROCA vulnerability or factorization using batch-GCD. We've collected over 300 million keys so far and built a database 4 to 10 times bigger than previous public works.

Performing the initial computation on over 300 million keys took about 10 days on a 280 vCPU cluster. Many optimizations allow our tool to incrementally test new RSA keys for common prime factors against the whole dataset in just a few minutes.

PRESENTATIONS

As a result of our research, we could have impersonated hundreds of people by breaking their PGP keys, mimicked thousands of servers thanks to their factored SSH keys and performed MitM attacks on over 200k websites relying on vulnerable X509 certificates.

In the end, we were able to do this in an entirely passive way. Going further is possible, but it would lead us to the dark side. Would big brother hesitate to go there?

FINDING XORI: MALWARE ANALYSIS TRIAGE WITH AUTOMATED DISASSEMBLY

Friday at 13:00 in Track 2
20 minutes | Demo, Tool

Amanda Rousseau
Senior Malware Researcher at Endgame Inc.

Rich Seymour
Senior Data Scientist at Endgame Inc

In a world of high volume malware and limited researchers we need a dramatic improvement in our ability to process and analyze new and old malware at scale. Unfortunately what is currently available to the community is incredibly cost prohibitive or does not rise to the challenge. As malware authors and distributors share code and prepackaged tool kits, the corporate sponsored research community is dominated by solutions aimed at profit as opposed to augmenting capabilities available to the broader community. With that in mind, we are introducing our library for malware disassembly called Xori as an open source project. Xori is focused on helping reverse engineers analyze binaries, optimizing for time and effort spent per sample.

Xori is an automation-ready disassembly and static analysis library that consumes shellcode or PE binaries and provides triage analysis data. This Rust library emulates the stack, register states, and reference tables to identify suspicious functionality for manual analysis. Xori extracts structured data from binaries to use in machine learning and data science pipelines.

We will go over the pain-points of conventional open source disassemblers that Xori solves,

examples of identifying suspicious functionality, and some of the interesting things we've done with the library. We invite everyone in the community to use it, help contribute and make it an increasingly valuable tool for researchers alike.

SYNFUZZ: BUILDING A GRAMMAR BASED RE-TARGETABLE TEST GENERATION FRAMEWORK

Friday at 10:00 in 101 Track, Flamingo
45 minutes | Demo, Tool

Joe Rozner
Hacker

Fuzzers have played an important role in the discovery of reliability and security flaws in software for decades. They have allowed for test case generation at a rate impossible by hand and the creation of test cases humans may never conceive of. While there are many excellent fuzzers available most are designed for mutating source files or input in random ways and attempting to discover edge cases in the handling of them. Some others are designed with structured input in mind and use grammars to more strategically generate and mutate possible inputs that adhere to the format defined. These specifically are the ones we care about for the goals of identifying differences between multiple implementations of a single language, finding bugs in parse tree generation/handling of tokens, and handling of the data at runtime once it has been successfully lexically and syntactically analyzed. We'll look at some of the shortcomings of existing fuzzers and discuss the implementation for a new platform designed to make fuzzer creation easier with the goal of being able utilize grammars from the implementations of the languages themselves.

BYPASSING PORT-SECURITY IN 2018: DEFEATING MACSEC AND 802.1X-2010

Friday at 15:00 in Track 1
45 minutes | Demo, Tool

Gabriel Ryan
Co-Founder / Principal Security Consultant @ Digital Silence

Existing techniques for bypassing wired port security are limited to attacking 802.1x-2004, which does not provide encryption or the ability to perform authentication on a packet-by-packet basis [1][2][3][4]. The development of 802.1x-2010 mitigates these issues by using MacSEC to provide Layer 2 encryption and packet integrity check to the protocol [5]. Since MacSEC encrypts data on a hop-by-hop basis, it successfully protects against the bridge-based attacks pioneered by the likes of Steve Riley, Abb, and Alva Duckwall [5][6].

In addition to the development of 802.1x-2010, improved 802.1x support by peripheral devices such as printers also poses a challenge to attackers. Gone are the days in which bypassing 802.1x was as simple as finding a printer and spoofing address, as hardware manufacturers have gotten smarter.

In this talk, we will introduce a novel technique for bypassing 802.1x-2010 by demonstrating how MacSEC fails when weak forms of EAP are used. Additionally, we will discuss how improved 802.1x support by peripheral devices does not necessarily translate to improved port-security due to the widespread use of weak EAP. Finally, we will consider how improvements to the Linux kernel have made bridge-based techniques easier to implement and demonstrate an alternative to using packet injection for network interaction. We have packaged each of these techniques and improvements into an open source tool called Silent Bridge, which we plan on releasing at the conference.

IN SOVIET RUSSIA SMARTCARD HACKS YOU

Saturday at 13:00 in Track 1
20 minutes | Demo, Tool, Exploit

Eric Sesterhenn
Principal Security Consultant at X41, D-Sec GmbH

The classic spy movie hacking sequence: The spy inserts a magic smartcard provided by the agency technicians into the enemy's computer, ...the screen unlocks... What we all laughed about is possible!

Smartcards are secure and trustworthy. This is the idea smartcard driver developers have in mind when developing drivers and smartcard software. The work presented in this talk not only challenges, but crushes this assumption by attacking smartcard drivers using malicious smartcards.

A fuzzing framework for *nix and Windows is presented along with some interesting bugs found by auditing and fuzzing smartcard drivers and middleware. Among them classic stack and heap buffer overflows, double frees, but also a replay attack against smartcard authentication.

Since smartcards are used in the authentication process, a lot of vulnerabilities can be triggered by an unauthenticated user, in code running with high privileges. During the authors research, bugs were discovered in OpenSC (EPass, PIV, OpenPGP, CAC, Cryptoflex,...), YubiKey drivers, pam_p11, pam_pkcs11, Apple smartcardservices...

- Identified vulnerabilities in various software projects including

the Linux kernel, X.org and multiple IoT Operating Systems

- Speaker at nullcon 2018, Internet of Teens (Issues in IoT Operating Systems)

- Speaker at 30C3 about fingerprinting Java web-applications (lightning talk).

- Part of the winning team of the Deutsche Post Security Cup 2013.

ALL YOUR MATH ARE BELONG TO US

Saturday at 15:00 in Track 1
45 minutes | Demo, Tool, Exploit, Audience Participation

sghotoma
Lead security researcher @ PR-Audit Ltd., Hungary

First of all, it's math. Not meth. So everybody be cool, I'm not gonna touch your central nervous system stimulant substances. Now that this is established, I can start telling my story. And this story, like all good stories, begins where it ends.

Wait, no, not really.

It begins at a birthday party where the sister of a friend asked if I could

help her with MATLAB. No matter how horrible memories I had about MATLAB, I just couldn't say no. So the next day, there was I, sitting in my room, installing the trial. And that's when the hacking started...

Believe me, there were a lot to hack in this case! Several gigabytes of installed materials, a few web servers, cloud integration, clustering capabilities, you name it. These software are bloated, they are basically their own little operating systems.

Yup, I used plural. Because I thought why discriminate MATLAB? I should really give a chance to Maple and Mathematica to fail too!. I did, and they did fail, and these failures gave the material for my talk. Basically this will be a dump of exploits (RCEs, file disclosures, etc.), and if you use any of those software and you are at least a bit security conscious, you should definitely listen to it.

HOUSE OF ROMAN: A "LEAKLESS" HEAP FENGSHUI TO ACHIEVE RCE ON PIE BINARIES

Saturday at 13:30 in 101 Track, Flamingo
20 minutes | Demo, Exploit

Sanat Sharma
Hacker

Regarding ptmalloc2, many heap exploitation techniques have been invented in the recent years, well documented on the famous how2heap repository, or as writeups of famous CTF challenges (like House of Orange). However, most of them require atleast a libc/heap leak, or fail in non-PIE binaries. My new technique titled House of Roman leverages a single bug to gain shell leaklessly on a PIE enabled Binary. I shall showcase the ease of aligning the heap to perform this attack, thus demonstrating its versatility.

Since this a 20 mins talk, attendees should be aware of basic heap exploitation techniques, like fastbin attacks and unsorted bin attacks, and have a general idea of how the ptmalloc2 algorithm works. As a bonus, I also discuss how to land a fastbin chunk in memory regions with no size alignment (like __free_hook).

UEFI EXPLOITATION FOR THE MASSES

Friday at 14:00 in 101 Track, Flamingo
45 minutes | Demo

Mickey Shkatov
Hacker

Jesse Michael
Hacker

So how do you debug bios and triage a vulnerability for exploitability with no stack trace or error log? How do BIOS developers do it? Do not worry! We will explain how anyone can have debug capabilities on modern Intel platforms and show you how this massively simplifies exploit dev. Developing an exploit for a BIOS vulnerability is a different experience than other types of exploit dev. Your available code base to draw from is unlike what you would expect when running at the operating system level and you have no gdb you can use.

In this talk we will summarize BIOS exploitation techniques and dive deeper into the specifics of an exploit we developed to provide reliable arbitrary code execution for an "over-the-internet" bios update vulnerability we found and responsibly disclosed. We will explain the relevant parts of UEFI and talk more about the exploit mitigations that exist there. We will also explain how to explore System Management Mode (SMM) in an Intel based platform, utilizing Intel hardware debug capabilities on an Intel 8th gen platform to obtain SMRAM content, analyze its contents, and search for vulnerable code.

FUZZING MALWARE FOR FUN & PROFIT: APPLYING COVERAGE-GUIDED FUZZING TO FIND AND EXPLOIT BUGS IN MODERN MALWARE

Sunday at 15:00 in Track 3
45 minutes | Demo, Tool, Exploit

Maksim Shudrak
Senior Offensive Security Researcher, Salesforce

Practice shows that even the most secure software written by the best engineers contain bugs. Malware is not an exception. In most cases their authors do not follow the best secure software development practices thereby introducing an interesting attack scenario which can be used to stop or slow-

PRESENTATIONS

down malware spreading, defend against DDoS attacks and take control over C&Cs and botnets. Several previous researches have demonstrated that such bugs exist and can be exploited. To find those bugs it would be reasonable to use coverage-guided fuzzing.

This talk aims to answer the following two questions: ___ we defend against malware by exploiting bugs in them ? How can we use fuzzing to find those bugs automatically ?

The author will show how we can apply coverage-guided fuzzing to automatically find bugs in sophisticated malicious samples such as botnet Mirai which was used to conduct one of the most destructive DDoS in history and various banking trojans. A new cross-platform tool implemented on top of WinAFL will be released and a set of 0day vulnerabilities will be presented.

Do you want to see how a small addition to HTTP-response can stop a large-scale DDoS attack or how a smart bitflipping can cause RCE in a sophisticated banking trojan? If the answer is yes, this is definitely your talk.

WAGGING THE TAIL: COVERT PASSIVE SURVEILLANCE AND HOW TO MAKE THEIR LIFE DIFFICULT

Thursday at 14:00 in 101 Track, Flamingo
45 minutes

Si
Independent Security Consultant

Agent X
Hacker

In this modern digital age of technically competent adversaries we forget that there may still be a need to conduct old school physical surveillance against a target. Many organisations utilise surveillance teams and these may be in-house in the case of government agencies or third-party teams contracted for a specific task and their targets range from suspected terrorists to people accused of bogus insurance claims.

Whilst most people think that they may never be placed under surveillance some professions increase this probability. For

example, if you are a member of the press with sources that you only meet face to face you could be a target especially if the source is a whistleblower or has information that their employer would rather they didn't give to you. Would it seem far-fetched to think that a hacker, security researcher or a member of the EFF could be placed under surveillance? Maybe even some current and former DEF CON speakers and attendees?

These teams are not the lone Private Investigator sat in their car at the bottom of your street but are highly trained individuals whose job is to remain undetected. Their mission is to observe and identify interactions and document everything they see. They aim to be "The Grey Man", that person, when asked to describe, you are unable to. Their techniques have changed very little over decades because they work.

This talk will focus on mobile and foot surveillance techniques used by surveillance teams. It will also include tips on identifying if you are under surveillance and how to make their life difficult.

PRACTICAL & IMPROVED WIFI MITM WITH MANA

Friday at 16:00 in Track 2
45 minutes | Demo, Audience Participation, Tool

singe
CTO @ SensePost

In 2014, we released the mana rogue AP toolkit at DEF CON 22. This fixed KARMA attacks which no longer worked against modern devices, added new capabilities such as KARMA against some EAP networks and provided an easy to use toolkit for conducting MitM attacks once associated.

Since then, several changes in wifi client devices, including MAC randomisation, significant use of the 5GHz spectrum and an increased variety of configurations has made these attacks harder to conduct. Just firing up a vanilla script gets fewer credentials than it used to.

To address this mana will be re-released in this talk with several significant improvements

to make it easier to conduct rogue AP MitM attacks against modern devices and networks.

After years of using mana in many security assessments, we've realised rogue AP'ing and MitM'ing is no simple affair. This extended talk will provide an overview of mana, the new capabilities and features, and walk attendees through three scenarios and their nuances:

- Intercepting corporate credentials at association (PEAP/EAP-GTC)
- Targeting one or more devices for MitM & collecting credentials
- "Snoopy" style geolocation & randomised MAC deanonymization As a bonus, you'll be able to download a training environment to practise all of this without requiring any wifi hardware (or breaking any laws).

JAILBREAKING THE 3DS THROUGH 7 YEARS OF HARDENING

Saturday at 11:00 in Track 3
45 minutes | Demo, Exploit

smea
Hacker

The 3DS was one of Nintendo's first serious attempts at security, featuring a cool microkernel based OS and actual exploit mitigations. That didn't stop it from getting hacked pretty hard, making it possible for people to write their own homebrew software for the console. But Nintendo isn't one to back off from a fight and, as a result, has put significant effort into not only fixing vulnerabilities but also introducing new security features targeted specifically at killing exploit techniques used by hackers. This talk will describe hacking the console through all these defensive features by walking through a 0-day exploit chain that takes us all the way from zero access to a full system jailbreak.

PRIVACY IS EQUALITY: AND IT'S FAR FROM DEAD

Saturday at 20:00-22:00 in Octavius 13
Fireside Hax

Sarah St. Vincent
Researcher/Advocate on National Security, Surveillance, and Domestic Law Enforcement, Human Rights Watch

A talk at DEF CON 25 claimed that privacy is "gone and never coming back." This talk offers a different

view, inviting the audience to see privacy as fundamentally about equality-something we have never fully had but also should never regard as gone. The speaker is a human rights lawyer and investigator, and will draw on decades of human rights thinking about state surveillance as well as her 2017 revelations about Defense Department monitoring of "homegrown violent extremists." Adopting a feminist and race-conscious perspective and inviting audience participation, the talk will challenge received wisdom about basic concepts such as privacy, national security, the warrant requirement, and online radicalization. With a view to the future, it will also offer a thought-provoking history of the connections between privacy and equality in the United States-and the ways unchecked surveillance operates to categorize us and reinforce divisions between us. It is easy to forget that _1984_ was partly a story about poverty and economic inequality. This talk embraces Orwell's insight into the connection between the erosion of privacy and a dangerous loss of equality, and carries it forward.

INSIDE THE FAKE SCIENCE FACTORY

Saturday at 16:00 in Track 3
105 minutes

Dr Cindy Poppins
Computer Scientist (AKA Svea Eckert)

Dr Dade Murphy
Reformed Hacker (AKA Suggy)

Professor Dr Edgar Munchhausen
Struwwelpeter Fellow (AKA Till Krause)

Fake News has got a sidekick and it's called Fake Science. This talk presents the findings and methodology from a team of investigative journalists, hackers and data scientists who delved into the parallel universe of fraudulent pseudo-academic conferences and journals; Fake science factories, twilight companies whose sole purpose is to give studies an air of scientific credibility while cashing in on millions of dollars in the process. Until recently, these fake science factories have remained relatively under the radar, with few outside of academia aware of their presence; but the highly profitable industry is growing significantly and with it, so

are the implications. To the public, fake science is indistinguishable from legitimate science, which is facing similar accusations itself. Our findings highlight the prevalence of the pseudo-academic conferences, journals and publications and the damage they can and are doing to society.

HACKING BLE BICYCLE LOCKS FOR FUN AND A SMALL PROFIT

Sunday at 14:00 in Track 2
45 minutes | Demo, Tool

Vincent Tan Kwang Yue
Senior Security Consultant, MWR InfoSecurity

Hack a lock and get free rides! (No free beer yet though...). This talk will explore the ever growing ride sharing economy and look at how the BLE "Smart" locks on shared bicycles work. The entire solution will be deconstructed and examined, from the mobile application to its supporting web services and finally communications with the lock. We will look at how to go about analysing communications between a mobile device and the lock, what works, what doesn't.

Previous talks on attacking BLE targeted the protocol itself using various hardware and software such as Ubertooth and Wireshark, which could be potentially difficult for someone new wanting to explore BLE and the ever connected IoT world. I'll simplify and stupidify the entire process such that anyone with a mobile phone and basic experience with Frida can go about breaking locks and hacking BLE the world over.

YOU CAN RUN, BUT YOU CAN'T HIDE. REVERSE ENGINEERING USING X-RAY.

Friday at 13:30 in 101 Track, Flamingo
20 minutes

George Tarnovsky
Engineer, Clsco Systems

Most of us have knowledge of PCB construction. In the past reversing someone's design was an easy task due to the simplicity of the PCB design. Now with BGA's (Ball Grid Array's), manufacturers using several plane layers cover the entire PCB

design and obscuring the details of the PCB from view. Thru the use of X-Ray, we are able to reverse engineer virtually anything. Slides will be presented show several PCB designs and how easy it was to reverse engineer the PCB. Also presenting videos of live views and dynamic zoom; this will demonstrate the true power of the X-Ray and its ability to see sub-micron features within the PCB structure and devices while manipulating the PCB.

WEAPONIZING UNICODE: HOMOGRAPHS BEYOND IDNS

Friday at 15:00 in 101 Track, Flamingo
45 minutes | Demo, Tool

The Tarquin
Senior Security Engineer, Amazon.com

Most people are familiar with homograph attacks due to phishing or other attack campaigns using Internationalized Domain Names with look-alike characters. But homograph attacks exist against wide variety of systems that have gotten far less attention. This talk discusses the use of homographs to attack machine learning systems, to submit malicious software patches, and to craft cryptographic canary traps and leak repudiation mechanisms. It then introduces a generalized defense strategy that should work against homograph attacks in any context.

THE ROAD TO RESILIENCE: HOW REAL HACKING REDEEMS THIS DAMNABLE PROFESSION

Saturday at 17:00 in Track 2
45 minutes |

Richard Thieme, a.k.a. neural cowboy
Author and professional speaker, ThiemeWorks

Two years ago Richard Thieme spoke on "Playing Through the Pain: The Impact of Dark Knowledge on Security and Intelligence Professionals" for Def Con 24. He relied on dozens of experiences provided by colleagues over a quarter-century, colleagues from NSA, CIA, corporate, and military. Responses to the presentation have often been emotional and have corroborated his thesis. The real impact of this work on people over the long term has to be mitigated by counter-measures and strategies

PRESENTATIONS

so scars can be endured or, even better, incorporated and put to use. In this presentation, Thieme elaborates those strategies and counter-measures. In what is likely his final speech at Def Con, he speaks directly to the “human in the machine” AS a human being. It’s not about leaving the profession: it’s about what we can do to thrive and transcend the challenges. It’s about “saving this space,” this play space of hacking, work and life, and knowing the cost of being fully human while encountering dehumanizing impacts. It is easier to focus on exploits, cool tools, zero days, and the games we play in the space that “makes us smile.” It is not so easy to know how to play through the pain successfully. The damage to us does not show up in brain scans. It shows up in our families, our relationships, and our lives. Thieme is not preaching, he is sharing insights based on what he too has had to transcend in his own life. They call a lot of us “supernormals,” which means we discovered resilient responses to deprivation, abuse, profound loss ... or the daily challenges of work that makes clear that evil is real. We are driven, we never quit, we fight through adversity, we create and recreate personas that work, we do what has to be done. It pays to know how we do that and know THAT we know so we can recreate resilience in the face of whatever comes our way. A contractor for NSA suggested that everyone inside the agency should see the video of “Playing Through the Pain.” A long-time Def Con attendee asks all new hires to watch “Staring into the Abyss,” a talk Thieme did a few years before. This subject matter is seldom discussed aloud “out here” and by all accounts is not taken seriously “inside,” which is perhaps why there have been half a dozen suicides lately at NSA and a CIA veteran said, “I have 23 suicides on my mind, the most recent senior people who could not live with what they knew.” The assumption baked into this talk: real hacking, its ethos and its execution, provides the tools we need to do this damn thing right.

This talk is in honor of Perry Barlow and the EFF.

BREAKING PASER LOGIC: TAKE YOUR PATH NORMALIZATION OFF AND POP 0DAYS OUT!

Friday at 12 in Track 2
45 minutes | [Demo](#), [Tool](#), [Exploit](#)

Orange Tsai
Security Researcher from DEVCORE

We propose a new exploit technique that brings a whole-new attack surface to defeat path normalization, which is complicated in implementation due to many implicit properties and edge cases. This complication, being underestimated or ignored by developers for a long time, has made our proposed attack vector possible, lethal, and general. Therefore, many 0days have been discovered via this approach in popular web frameworks written in trending programming languages, including Python, Ruby, Java, and JavaScript.

Being a very fundamental problem that exists in path normalization logic, sophisticated web frameworks can also suffer. For example, we’ve found various 0days on Java Spring Framework, Ruby on Rails, Next.js, and Python aiohttp, just to name a few. This general technique can also adapt to multi-layered web architecture, such as using Nginx or Apache as a proxy for Tomcat. In that case, reverse proxy protections can be bypassed. To make things worse, we’re able to chain path normalization bugs to bypass authentication and achieve RCE in real world Bug Bounty Programs. Several scenarios will be demonstrated to illustrate how path normalization can be exploited to achieve sensitive information disclosure, SMB-Relay and RCE.

Understanding the basics of this technique, the audience won’t be surprised to know that more than 10 vulnerabilities have been found in sophisticated frameworks and multi-layered web architectures aforementioned via this technique.

COMPROMISING ONLINE ACCOUNTS BY CRACKING VOICEMAIL SYSTEMS

Friday at 13:00 in Track 1
20 minutes | [Demo](#), [Audience Participation](#), [Tool](#)

Martin Vigo
Hacker

Voicemail systems have been with us since the 80s. They played a big role in the earlier hacking scene and re-reading those e-zines, articles and tutorials paints an interesting picture. Not much has changed. Not in the technology nor in the attack vectors. Can we leverage the last 30 years innovations to further compromise voicemail systems? And what is the real impact today of pwning these?

In this talk I will cover voicemail systems, it’s security and how we can use oldskool techniques and new ones on top of current technology to compromise them. I will discuss the broader impact of gaining unauthorized access to voicemail systems today and introduce a new tool that automates the process.

ATTACKING THE MACOS KERNEL GRAPHICS DRIVER

Sunday at 12:00 in Track 2
45 minutes | [Demo](#), [Exploit](#)

Yu Wang
Senior Staff Engineer at Didi Research America

Just like the Windows platform, graphic drivers of macOS kernel are complicated and provide a large promising attack surface for EoPs and sandbox escapes from low-privileged processes. After auditing part of the binaries, I discovered a number of vulnerabilities last year. Including, NULL pointer dereference, stack-based buffer overflow, arbitrary kernel memory read and write, use-after-free, etc. Some of these vulnerabilities were reported to Apple Inc., such as the CVE-2017-7155, CVE-2017-7163, CVE-2017-13883.

In this presentation, I will share with you the detailed information about these vulnerabilities. Furthermore, from the attacker’s perspective, I will also reveal some new exploit techniques and zero-days.

FIRE & ICE: MAKING AND BREAKING MACOS FIREWALLS

Saturday at 14:30 in Track 3
20 minutes | [Demo](#), [Tool](#), [Exploit](#)

Patrick Wardle
Chief Research Officer, Digita Security

In the ever raging battle between malicious code and anti-malware tools, firewalls play an essential

role. Many a malware has been generically thwarted thanks to the watchful eye of these products.

However on macOS, firewalls are rather poorly understood. Apple’s documentation surrounding it’s network filter interfaces is rather lacking and all commercial macOS firewalls are closed source.

This talk aims to take a peek behind the proverbial curtain revealing how to both create and ‘destroy’ macOS firewalls.

In this talk, we’ll first dive into what it takes to create an effective firewall for macOS. Yes we’ll discuss core concepts such as kernel-level socket filtering—but also how to communicate with user-mode components, install privileged code in a secure manner, and simple ways to implement self-defense mechanisms (including protecting the UI from synthetic events).

Of course any security tool, including firewalls, can be broken. After looking at various macOS malware specimens that proactively attempt to detect such firewalls, we’ll don our ‘gray’ (black?) hats to discuss various attacks against these products. And while some attacks are well known, others are currently undisclosed and can generically bypass even today’s most vigilant Mac firewalls.

But all is not lost. By proactively discussing such attacks, combined with our newly-found understandings of firewall internals, we can improve the existing status quo, advancing firewall development. With a little luck, such advancements may foil, or at least complicate the lives of tomorrow’s sophisticated Mac malware!

THE MOUSE IS MIGHTIER THAN THE SWORD

Sunday at 10:00 in 101 Track, Flamingo
45 minutes | [Demo](#), [Exploit](#)

Patrick Wardle
Chief Research Officer, Digita Security

In today’s digital world the mouse, not the pen is arguably mightier than the sword. Via a single click, countless security mechanisms may be completely bypassed. Run untrusted app? click ...allowed. Authorize keychain access? click ...allowed.

Load 3rd-party kernel extension? click ...allowed. Authorize outgoing network connection? click ...allowed. Luckily security-conscious users will (hopefully) heed such warning dialogues—stopping malicious code in its tracks. But what if such clicks can be synthetically generated and interact with such prompts in a completely invisible way? Well, then everything pretty much goes to hell.

Of course OS vendors such as Apple are keenly aware of this ‘attack’ vector, and thus strive to design their UI in a manner that is resistant against synthetic events. Unfortunately they failed.

In this talk we’ll discuss a vulnerability (CVE-2017-7150) found in all recent versions of macOS that allowed unprivileged code to interact with any UI component including ‘protected’ security dialogues. Armed with the bug, it was trivial to programmatically bypass Apple’s touted ‘User-Approved Kext’ security feature, dump all passwords from the keychain, bypass 3rd-party security tools, and much more! And as Apple’s patch was incomplete (surprise surprise) we’ll drop an 0day that (still) allows unprivileged code to post synthetic events and bypass various security mechanisms on a fully patched macOS box!

And while it may seem that such synthetic interactions with the UI will be visible to the user, we’ll discuss an elegant way to ensure they happen completely invisibly!

WELCOME TO DEF CON & BADGE MAKER TALK

Friday at 10:00 in Track 1
45 minutes | [Demo](#)

The Dark Tangent

BARCOWNED: POPPING SHELLS WITH YOUR CEREAL BOX

Sunday at 13:00 in Track 3
20 minutes | [Demo](#)

Michael West
Technical Advisor at CyberArk

magicspacekiwi (Colin Campbell)
Web Developer

Barcodes and barcode scanners are ubiquitous in many industries and work with untrusted data on labels, boxes, and even phone screens. Most

scanners also allow programming via barcodes to manipulate and inject keystrokes. See the problem? By scanning a few programming barcodes, you can infect a scanner and access the keyboard of the host device, letting you type commands just like a Rubber Ducky. This culminates in barcOwned—a small web app that allows you to program scanners and execute complex, device-agnostic payloads in seconds. Possible applications include keystroke injection (including special keys), infiltration and exfiltration of data on air-gapped systems, and good ol’ denial of service attacks.

DISRUPTING THE DIGITAL DYSTOPIA OR WHAT THE HELL IS HAPPENING IN COMPUTER LAW?

Friday at 20:00-22:00 in Octavius 13
Fireside Hax | [Audience Participation](#)

Nathan White
Senior Legislative Manager, Access Now

Nate Cardozo
Senior Staff Attorney, EFF

1984 didn’t just happen because of a calendar. The world of 1984 was built by politicians who used the rule of law to change society into an oppressive surveillance state. In Washington D.C., politicians today are making decisions about what technologies we’re permitted to use and how they’ll be used in society. In this talk we’ll break down 4-5 bills currently under discussion in Congress and explain who they’ll impact the DEF CON community.

BETRAYED BY THE KEYBOARD: HOW WHAT YOU TYPE CAN GIVE YOU AWAY

Sunday at 14:00 in 101 Track, Flamingo
45 minutes

Matt Wixey
Vulnerability R&D Lead, PwC

Attribution is hard. Typically, the most useful identifiers—IP addresses, email address, domains, and so on—are also the easiest things to spoof, obfuscate, or anonymise. Whilst more advanced techniques, such as correlating malicious activity with timezones, or linking attacks through the use of similar techniques or malware, can be

PRESENTATIONS

useful, they tend to take investigators further away from the individuals responsible; at best, some inference about the country or specific actor group/collective can be made.

In this talk, I present a method for linking incidents to individual attackers with a high degree of accuracy, based on extremely fine-grained behavioural characteristics. This involves an investigatory technique known as “case linkage analysis” (CLA), which uses granular aspects of crime scene behaviours to link common offenders together through statistical comparison. It’s been applied to some crime types before, but never to cyber attacks.

I’ll cover how CLA works, its advantages and disadvantages, and how it has previously been applied to a range of crimes, from burglary to homicide. I’ll place it within the context of personality psychology, biometrics, forensic criminology, offender profiling, and forensic linguistics; and will walk through applying it practically.

I’ll then show the results of a novel experiment I conducted applying CLA to network intrusion attacks, which involved logging the keystrokes of volunteer attackers across different simulated intrusions, breaking these down into specific behaviours and syntax, and using these to link individuals to their offences. The end result: the way you type commands, including your choice and order of syntax, switches, and options, can form distinctive behavioural signatures, which can be used to link attackers together. Linking accuracy rates as high as 99% were achieved.

Finally, I’ll talk about the implications for both defenders and everyone else (particularly focusing on the privacy implications), explore ways in which these techniques could be defeated, and outline some ideas for future research in these areas.

HACKING THE BRAIN: CUSTOMIZE EVIL PROTOCOL TO PWN AN SDN CONTROLLER

Friday at 13:30 in Track 2
20 minutes | Demo, Exploit

Feng Xiao
Hacker

Jianwei Huang
Hacker

Peng LiuRaymond G. Tronzo, M.D.
Professor of Cybersecurity

Software-Defined Networking (SDN) is now widely deployed in production environments with an ever-growing community. Though SDN’s software-based architecture enables network programmability, it also introduces dangerous code vulnerabilities into SDN controllers. However, the decoupled SDN control plane and data plane only communicate with each other with pre-defined protocol interactions, which largely increases the difficulty of exploiting such security weaknesses from the data plane.

In this talk, we extend the attack surface and introduce Custom Attack, a novel attack against SDN controllers that leverages legitimate SDN protocol messages (i.e., the custom protocol field) to facilitate Java code vulnerability exploitation. Our research shows that it was possible for a weak adversary to execute arbitrary command or manipulate data in the SDN controller without accessing the SDN controller or any applications, but only controlling a host or a switch.

To the best of our knowledge, Custom Attack is the first attack that can remotely compromise SDN software stack to simultaneously cause multiple kinds of attack effects in SDN controllers. Till now we have tested 5 most popular SDN controllers and their applications and found all of them are vulnerable to Custom Attack in some degree. 14 serious vulnerabilities are discovered, all of which can be exploited remotely to launch advanced attacks against controllers (e.g., executing arbitrary commands, exfiltrating confidential files, crashing SDN service, etc.).

This presentation will include:

1. an overview of SDN security research and practices.
2. a new attack methodology for SDN that is capable of compromising the entire network.
3. our research process that leads to these discoveries, including technical specifics of exploits.

4. showcases of interesting Custom Attack chains in real-world SDN projects.

PRIVACY INFRASTRUCTURE, CHALLENGES AND OPPORTUNITIES

Friday at 15:00 in Track 3
45 minutes

yawnbox
Executive Director, Emerald Onion

We started our own transit Internet Service Provider (ISP) to safely route anonymized packets across the globe, and you can too. Emerald Onion is a Seattle-based 501(c)3 not-for-profit and we want to help other hacker collectives start their own. Getting your own Autonomous System Number (ASN), managing Internet Protocol (IP) scopes, using Border Gateway Protocol (BGP) in Internet Exchange Points (IXPs), dealing with abuse complaints or government requests for user data—this is all stuff that you can do. Not every technologist is comfortable with launching and managing a nonprofit organization let alone has all of the technical knowhow to run an ISP. We didn’t either when we started. We had a goal, and that was to route unfiltered Tor exit traffic in the Seattle Internet Exchange despite National Security Agency (NSA) wiretaps in the Westin Exchange Building. This talk will cover high level challenges and opportunities surrounding privacy infrastructure in the United States.

INFECTING THE EMBEDDED SUPPLY CHAIN

Saturday at 13:30 in Track 3
45 minutes | Demo, Exploit

Zach
Security Researcher at Somerset Recon

Alex
Security Researcher at Somerset Recon

With a surge in the production of internet of things (IoT) devices, embedded development tools are becoming commonplace and the software they run on is often trusted to run in escalated modes. However, some of the embedded development tools on the market contain serious vulnerabilities that put users at risk. In this talk we discuss the various

attack vectors that these embedded development tools expose users to, and why users should not blindly trust their tools. This talk will detail a variety reverse engineering, fuzzing, exploit development and protocol analysis techniques that we used to analyze and exploit the security of a common embedded debugger.

LORA SMART WATER METER SECURITY ANALYSIS

Friday at 11:00 in Track 3
45 minutes | Tool

Yingtao Zeng
Security Researcher at UnicornTeam, Radio Security Research Department of 360 Security Technology

Lin Huang
Senior Wireless Security Researcher and SDR technology expert, 360 Security Technology

Jun Li
Senior Security Researcher, Radio Security Department of 360 Security Technology

To avoid the tedious task of collecting water usage data by go user’s home _water meters that are equipped with wireless communication modules are now being put into use, in this talk we will take a water meter _which is using Lora wireless protocol_ as an example to analyze the security and privacy risks of this kind of meters_ we will explain how to reverse engineer and analyze both the firmware and the hardware of a water meter system, we will be talking about its security risks from multiple perspectives , physical, data link, and sensors. Do notice that LORA is not only used in water meter ,it is being used in a lot of IoT scenarios _so the methods we employed to analyze LORA in this talk are also useful when you do tests of other LORA based systems.

DISSECTING THE TEDDY RUXPIN: REVERSE ENGINEERING THE SMART BEAR

Friday at 13:00 in 101 Track, Flamingo
20 minutes | Demo, Audience Participation, Tool

zenofex
Hacker

The Teddy Ruxpin is an iconic toy from the 1980’s featuring an animatronic teddy bear that reads stories from cassette tapes to children. In late 2017, a new

model of the toy was released with improvements including Bluetooth connectivity, LCD eyes, and a companion mobile application. While the new bear features a number of improvements, the Teddy Ruxpin’s original ability to add new stories by replacing the included cassettes is no longer applicable, and it requires users to supply files to the bear in a proprietary format.

This presentation aims to show how the new Teddy Ruxpin was reverse engineered down to a very low level in order to create new content. I will reveal the inner workings of the hardware and software within the bear and document the process used to reverse engineer it. I will then examine the communication between the mobile application and Teddy Ruxpin as well as the custom structure of the digital books read by the bear. I will end the presentation by releasing a toolset that allows users to create their own stories followed by a demo showcasing the Teddy Ruxpin greeting the DEF CON audience.

DEMYSTIFYING MS17-010: REVERSE ENGINEERING THE ETERNAL EXPLOITS

Sunday at 11:00 in Track 3
45 minutes | Demo, Tool, Exploit, Audience Participation

zerosum0x0
Hacker

MS17-010 is the most important patch in the history of operating systems, fixing remote code execution vulnerabilities in the world of modern Windows. The ETERNAL exploits, written by the Equation Group and dumped by the Shadow Brokers, have been used in the most damaging cyber attacks in computing history: WannaCry, NotPetya, Olympic Destroyer, and many others.

Yet, how these complicated exploits work has not been made clear to most. This is due to the ETERNAL exploits taking advantage of undocumented features of the Windows kernel and the esoteric SMBv1 protocol.

This talk will condense years of research into Windows internals and the SMBv1 protocol driver. Descriptions of full reverse

engineering of internal structures and all historical background info needed to understand how the exploit chains for ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY work will be provided.

This talk will also describe how the MS17-010 patch fixed the vulnerabilities, and identify additional vulnerabilities that were patched around the same time.

FASTEN YOUR SEATBELTS: WE ARE ESCAPING IOS 11 SANDBOX!

Friday at 13:30 in Track 3
20 minutes | Demo, Exploit

Min (Spark) Zheng
Security Expert, Alibaba Inc.

Xiaolong Bai
Security Engineer, Alibaba Inc.

Apple’s sandbox was introduced as “SeatBelt” in macOS 10.5 which provided the first full-fledged implementation of the MACF policy. After a successful trial on macOS, Apple applied sandbox mechanism to iOS 6. In its implementation, the policy hooked dozens of operations. The number of hooks has been growing steadily when new system calls or newly discovered threats appeared. In the beginning, Apple’s sandbox used a black list approach which means Apple originally concentrated on the known dangerous APIs and blocked them, allowing all others by default. However, with the evolution of Apple’s sandbox, it applies a white list approach that denies all APIs and only allows secure ones that Apple trusts.

In this talk, we will first introduce Apple’s sandbox mechanism and profiles in the latest iOS. Then, we discuss iOS IPC mechanism and review several old classic sandbox escape bugs. Most importantly, we show two new zero-day sandbox escape vulnerabilities we recently discovered in the latest iOS 11.4. Besides, we share our experience of exploiting vulnerabilities in system services through OOL msg heap spray and ROP (Return-oriented programming). In addition,

we discuss a task port exploit technique which can be used to control the whole remote process through Mach messages. By using these techniques, security researchers could find and exploit sandbox escape bugs to control iOS user mode system services and further attack the kernel.

YOUR PERIPHERAL HAS PLANTED MALWARE: AN EXPLOIT OF NXP SOCS VULNERABILITY

Friday at 16:00 in Track 1
45 minutes | Demo, Exploit

Yuwei Zheng
Senior Security Researcher, Unicorn Team, 360 Technology

Shaokun Cao
Freelance Security Researcher

Yunding Jian
Senior Security Researcher, Unicorn Team, 360 Technology

Mingchuang Qun
Senior security researcher at the Radio Security Research Department of 360 Technology,

There are billions of ARM Cortex M based SOC being deployed in embedded systems. Most of these devices are Internet ready and definitely security is always the main concern. Vendors would always apply security measurements into the ARM Cortex M product for few major reasons: 1) People will not be able to copy and replicate the product; 2) License control for the hardware and software; 3) Prevent malicious code injection in to the firmware. Vendors normally rely on the security measurements built within the chip (unique ID number/ signature) or security measurements built around the chip (secure boot).

In this talk, we will share the ARM Cortex M SOC vulnerability that we discovered and it will be two parts:

The first is security measurement build within the SOC and how we break it. We could gain control of changing the SOC unique ID and write the firmware or even turn the device into a trojan or bot.

The second is security measure built around the SOC and how we break the Secure Boot elements and write into the firmware.

POLITICS AND THE SURVEILLANCE STATE. THE STORY OF A YOUNG POLITICIAN'S SUCCESSFUL EFFORTS TO FIGHT SURVEILLANCE AND PASS THE NATION'S STRONGEST PRIVACY BILLS.

Sunday at 11:00 in Track 2
45 minutes | Audience Participation

Daniel Zolnikov
Montana State Representative

Orwell's concept of 1984 has more to do with government misuse of technology than technology itself. New technology allows for more opportunity, but unchecked, it allows for complete government control.

Representative Daniel Zolnikov is the nation's leading politician regarding privacy and surveillance and has enacted numerous laws safeguarding fourth amendment rights regarding digital communications and technology. Daniel will walk you down the road of how political misuse of technology can and will turn the Federal Government into an unprecedented nanny state that will lead to a suppressed free flow of information and fear of stepping out of line. His story includes insights on how unique left and right coalitions were formed to pass these laws in his home state of Montana, and how he prevailed against law enforcement groups who opposed implementing warrant requirements.

This discussion is aimed at sharing insights no matter your political affiliation. All of Daniel's legislation has passed with overwhelming bi-partisan support through both bodies in Montana's legislature and was signed by the governor of the opposite party. Although most speeches involving politicians tend to lead towards rhetoric, Daniel's goal is to share enough information to be able to understand why change has not taken place yet, and leave you understanding how to remedy that.

His story will give you insights into the politics that states and the nation face when reforming these issues, and his down to earth approach will bring the topic down to a level of humor and easy understanding.

There is no need for any technical or political insight to be able to appreciate this topic and the work Daniel has done on behalf of the more technologically savvy enthusiasts.

The theme of DEF CON 26 would be inconsistent without taking into consideration policy and how it ties in closely with technology. Technology relies on policy, and policy has the implications of dictating the use of technology. The two can go hand in hand, or end up squaring up against each other. You are an important, and lesser heard voice in the world of aged politicians with limited vision. The Orwellian state existed due to a mixture of bad policies and technology. Although the theme focuses on technology used to disrupt the surveillance state, the other half of the battle is ensuring this state does not reach the disastrous conclusions of 1984.

Daniel believes we can move forward with technology without living in fear of our government. If you want to have some hope and direction towards the future of policy regarding surveillance and technology, Daniel will leave you with the optimism that there is still a chance that our nation can have a balanced approach that ensures 1984 does not become the norm in the future and will help you understand how to take part in this action.

WORKSHOPS

WORKSHOP REGISTRATION WAS HELD ONLINE JULY 8TH. THERE IS NO ONSITE REGISTRATION, SIGNUP SHEET, AND ALL SEATS (INCLUDING STANDBY) ARE SOLD OUT. FOR MORE INFO ON THE WORKSHOPS VISIT THE DEF CON WEBSITE. PRE-REGISTRATION WILL BE ONLINE AGAIN FOR DEF CON 27!

THURSDAY

	ICON A	ICON B	ICON C	ICON D	ICON E	ICON F
10:00-14:00	Guided Tour to IEEE 802.15.4 and BLE Exploitation Arun Mane & Rushikesh D. Nandedkar	Pentesting ICS 101 Alexandrine Torrents & Arnaud SOULLIÉ	Where's My Browser? Learn Hacking iOS and Android Web-Views David Turco & Jon Overgaard Christiansen	Finding Needles in Haystacks Louis Nyffenegger & Luke Jahnke	Building Autonomous AppSec Test Pipelines with the Robot Framework Abhay Bhargav & Sharath Kumar Ramadas	Packet Mining for Privacy Leakage Dave Porcello & Sean Gallagher
14:30-18:30	Forensic Investigation for the Non-Forensic Investigator Gary Bates	Introduction to Cryptographic Attacks Matt Cheung	Advanced Wireless Attacks Against Enterprise Networks Gabriel Ryan & Justin Whitehead	Fuzzing FTW Bryce Kunz & Kevin Lustic	Playing with RFID Vinnie Vanhoeff & Lorenzo Bernardi	The Truth is in the Network David Pearson

FRIDAY

	ICON A	ICON B	ICON C	ICON D	ICON E	ICON F
10:00-14:00	Bypassing Windows Driver Signature Enforcement Csaba Fítl	Reverse Engineering with Open-SCAD and 3D Printing Nick Tait	Attacking Active Directory and Advanced Defense Methods in 2018 Adam Steed & James Albany	ARM exploitation 101 Sneha Rajguru	Attacking & Auditing Docker Containers Using Open Source Madhu Akula	Crypto Hero Sam Bowne, Dylan James Smith, & Elizabeth Biddlecome
14:30-18:30	Hacking Thingz Powered By Machine Learning Clarence Chio & Anto Joseph	Buzzing Smart Devices: Smart Band Hacking Arun Magesh	Threat Hunting with ELK Ben Hughes, Fred Mastrippolito, & Jeff Magloire	JWAT...Attacking JSON Web Tokens Louis Nyffenegger & Luke Jahnke	Penetration Testing Environments: Client & Test Security Wesley McGrew & Kendall Blaylock	Deploying, Attacking, and Securing Software Defined Networks Jon Medina

SATURDAY

	ICON A	ICON B	ICON C	ICON D	ICON E	ICON F
10:00-14:00	Joe Grand's Hardware Hacking Basics Joe Grand	Fuzzing with AFL (American Fuzzy Lop) Jakub Botwicz & Wojciech Rauner	Advanced Custom Network Protocol Fuzzing Joshua Pereyda & Timothy Clemans	Adventures in Radio Scanning Richard Henderson & Bryan Passifiume	Attack & Defense in AWS Environments Vaibhav Gupta & Sandeep Singh	Decentralized Hacker Net Eijah
14:30-18:30	Build Your Own OpticSpy Receiver Module Joe Grand	Weapons Training for the Empire Jeremy Johnson	Building Environmentally Responsive Implants with Gscript Vyrus, Dan Borges, & Alex Levinson	Lateral Movement 101: 2018 Update Walter Cuestas & Mauricio Velazco	Analyzing Malscripts: Return of the Exploits! Sergei Frankoff & Sean Wilson	Securing Big Data in Hadoop Miguel Guirao

#WIFICACTUS

Saturday 08/11/18 from 1000-1150 at Table One

Offense, defense, hardware

Mike Spicer

The newly upgraded #WiFiCactus for DEF CON 26 is a passive wireless monitoring backpack that listens to 60 channels of 2.4 and 5 GHz WiFi at the same time. New this year is the ability to capture 802.11AC traffic and upgrades to remove bandwidth bottlenecks. This tool uses Kismet to capture the data from the each radio and aggregates them into a single searchable web interface. This tool is also capable of identifying wireless threats, troubleshooting complex wireless environments and helping with correlation analysis between Bluetooth and WiFi.

<http://palshack.org/the-hashtag-wifi-cactus-wificactus-def-con-25/>

ADRECON: ACTIVE DIRECTORY RECON

Saturday 08/11/18 from 1200-1350 at Table Six

Security professionals (Blue Team, Red Team), system administrators, etc.

Prashant Mahajan

ADRecon is a tool which extracts various artifacts (as highlighted below) out of an AD environment in a specially formatted Microsoft Excel report that includes summary views with metrics to facilitate analysis. The report can provide a holistic picture of the current state of the target AD environment. The tool is useful to various classes of security professionals like system administrators, security professionals, DFIR, etc. It can also be an invaluable post-exploitation tool for a penetration tester. It can be run from any workstation that is connected to the environment, even hosts that are not domain members. Furthermore, the tool can be executed in the context of a non-privileged (i.e. standard domain user) accounts. Fine Grained Password Policy, LAPS and BitLocker may require Privileged user accounts. The tool will use Microsoft Remote Server Administration Tools (RSAT) if available, otherwise it will communicate with the Domain Controller using LDAP.

The following information is gathered by the tool: Forest; Domain; Trusts; Sites; Subnets; Default Password Policy; Fine Grained Password Policy (if implemented); Domain Controllers, SMB versions, whether SMB Signing is supported and FSMO roles; Users and their attributes; Service Principal Names (SPNs); Groups and memberships; Organizational Units (OUs); ACLs for the Domain, OUs, Root Containers and GroupPolicy objects; Group Policy Object details; DNS Zones and Records; Printers; Computers and their attributes; LAPS passwords (if implemented); BitLocker Recovery Keys (if implemented); and GPOResult (requires RSAT).

<https://github.com/sense-of-security/ADRecon>

ANGAD: A MALWARE DETECTION FRAMEWORK USING MULTI-DIMENSIONAL VISUALIZATION

Saturday 08/11/18 from 1600-1750 at Table Two

Defense, Forensics, Network, Malware

Ankur Tyagi

Angad is a framework to automate classification of an unlabelled malware dataset using multi-dimensional modelling. The input dataset is analyzed to collect various attributes which are then arranged in a number of feature vectors. These vectors are then individually visualized, indexed and then queried for each new input file. Matching vectors are labelled as per their AV detection categories for now but this could be changed to a heuristics approach if needed. If dynamic behavior or network traffic details are available, vectors are also converted into activity graphs that depict evolution of activity with a predefined time scale. This results into an animation of malware/malware category's behavior traits and is also useful in identifying activity overlaps across the input dataset.

Malware detection is a challenging task as the landscape is ever-evolving. Every other day, a new variant or a known malware family is reported and signature driven tools race against time to add detection. The process worsens when the rate of incoming samples is in thousands on a daily basis, making static/dynamic analysis alone of no use.

Angad tries to address this issue by leveraging well-known data classification techniques to the malware domain. It tries to provide a known interface to the multi-dimensional modelling approach within a standalone package.

<https://github.com/7h3rAm/angad>

ARCHERY: OPEN SOURCE VULNERABILITY ASSESSMENT AND MANAGEMENT

Saturday 08/11/18 from 1000-1150 at Table Two

Offense

Anand Tiwari

Archery is an opensource vulnerability assessment and management tool which helps developers and pentesters to perform scans and manage vulnerabilities. Archery uses popular opensource tools to perform comprehensive scanning for web application and network. It also performs web application dynamic authenticated scanning and covers the whole applications by using selenium. The developers can also utilize the tool for implementation of their DevOps CI/CD environment.

<https://github.com/archerysec/archerysec/>

BLEMYSTIQUE: AFFORDABLE CUSTOM BLE TARGET

Saturday 08/11/18 from 1200-1350 at Table Five

Attack and Defence

Nishant Sharma, Jeswin Mathai

BLEMystique is an ESP32 based custom BLE target which can be configured by the user to behave like one of the multiple BLE devices. BLEMystique allows a pentester to play with the BLE side of different kind of smart devices with a single piece of affordable ESP32 chip. BLEMystique contains multiple device profiles, for example, Smart Lock, Smart health band, Smart bulb, Heart rate monitor, Smart Bottle and more.

The BLEMystique code and manuals will be released to general public. So, apart from using the pre-configured devices, the users can also add support for devices for their choice and use their ESP32 board for target practice. In this manner, this tool can improve the overall experience of learning BLE pentesting.

BOOFUZZ

Saturday 08/11/18 from 1600-1750 at Table Five

Vulnerability Analysis, AppSec, Offense.

Joshua Pereyda

boofuzz is an open source network protocol fuzzing framework, competing with closed source commercial products like Defensics and Peach.

Inheriting from the open source tools Spike and Sulley, boofuzz improves on a long line of block-based fuzzing frameworks.

The framework allows hackers to specify protocol formats, and boofuzz does the heavy lifting of generating mutations specific to the format. boofuzz makes developing protocol-specific "smart" fuzzers relatively easy. Make no mistake, designing a smart network protocol fuzzer is no trivial task, but boofuzz provides a solid foundation for producing quality fuzzers.

Written in Python, boofuzz builds on its predecessor, Sulley, with key features including:

- Online documentation.
- More extensibility including support for arbitrary communications mediums.
- Built-in support for serial fuzzing, ethernet- and IP-layer, UDP broadcast.
- Much easier install experience!
- Far fewer bugs.

<https://github.com/jtpereyda/boofuzz>

CHIRON

Sunday 08/12/18 from 1000-1150 at Table Three

Defense

Rod Soto, Joseph Zadeh

Home-based open source network analytics and machine learning threat detection.

CHIRON is a home analytics based on ELK stack combined with Machine Learning threat detection framework AKTAION. CHIRON parses and displays data from POf, Nmap, and BRO IDS. CHIRON is designed for home use and will give great visibility to

home internet devices (IOT, Computers, Cellphones, Tablets, etc). CHIRON is integrated with AKTAION which detects exploit delivery ransomware/phishing.

<https://github.com/jzadeh/chiron-elk>

CLOUD SECURITY SUITE: ONE STOP TOOL FOR AWS, GCP & AZURE SECURITY AUDIT

Saturday 08/11/18 from 1200-1350 at Table Two

Defense, Cloud professionals

Jayesh Singh Chauhan

Nowadays, cloud infrastructure is pretty much the de-facto service used by large/small companies. Most of the organisations have partially or entirely moved to cloud. With more and more companies moving to cloud, the security of cloud becomes a major concern.

While AWS, GCP & Azure provide you protection with traditional security methodologies and have a neat structure for authorisation/configuration, their security is as robust as the person in-charge of creating/assigning these configuration policies. We all know, human error is inevitable and any such human mistake could lead to catastrophic damage to the environment.

Knowing this, audit of cloud infrastructure becomes a hectic task! There are a few open source tools which help in cloud auditing but none of them have an exhaustive checklist. Also, collecting, setting up all the tools and looking at different result sets is a painful task. Moreover, while maintaining big infrastructures, system audit of server instances is a major task as well.

CS Suite is a one stop tool for auditing the security posture of the AWS/GCP/Azure infrastructures and does OS audits as well. CS Suite leverages current open source tools capabilities and has custom checks added into one tool to rule them all.

<https://github.com/SecurityFTW/cs-suite>

CONFORMER

Sunday 08/12/18 from 1000-1150 at Table Six

Offense, AppSec

Mikhail Burshteyn

Conformer is a penetration testing tool, mostly used for external assessments to perform password based attacks against common webforms. Conformer was created from a need for password guessing against new web forms, without having to do prior burp work each time, and wanting to automate such attacks. Conformer is modular with many different parameters and options that can be customized to make for a powerful attack. Conformer has been used in countless assessments to obtain valid user credentials for accessing the internal environment through VPN, other internal resources or data to further the assessment.

<https://github.com/mikhhur/conformer>

DEJAVU: AN OPEN SOURCE DECEPTION FRAMEWORK

Sunday 08/12/18 from 1200-1350 at Table Three

Offense/Defense

Bhadreshkumar Patel, Harish Ramadoss

Deception techniques—if deployed well—can be very effective for organizations to improve network defense and can be a useful arsenal for blue teams to detect attacks at very early stage of cyber kill chain. But the challenge we have seen is deploying, managing and administering decoys across large networks. Although there are lot of commercial tools in this space, we haven't come across open source tools which can achieve this.

With this in mind, we have developed DejaVu which is an open source deception framework which can be used to deploy, configure and administer decoys centrally across the infrastructure. A web-based management console can be used by the defender to deploy multiple interactive decoys (HTTP Servers, SQL, SMB, FTP, SSH, client side-NBNS) strategically across their network on different VLANs. Logging and alerting dashboard displays detailed information about the alerts generated and can be further configured to generate high accuracy alert; and how these alerts should be handled.

Decoys can also be placed on the client VLANs to detect client side attacks such as responder/LLMNR attacks using client side decoys. Additionally, common attacks which the adversary uses to compromise such as abusing Tomcat/SQL server for initial foothold can be deployed as decoys, luring the attacker and enabling detection.

<https://github.com/bhadresh/Dejavu>

EAPHAMMER

Saturday 08/11/18 from 1400-1550 at Table One

Offensive security professionals, red teamers, penetration testers, researchers.

Gabriel Ryan

EAPHammer is a toolkit for performing targeted evil twin attacks against WPA2-Enterprise networks. It is designed to be used in full scope wireless assessments and red team engagements. As such, focus is placed on providing an easy-to-use interface that can be leveraged to execute powerful wireless attacks with minimal manual configuration. To illustrate how fast this tool is, here's an example of how to setup and execute a credential stealing evil twin attack against a WPA2-EAP network in just two commands:

```
# generate certificates
./eaphammer --cert-wizard
# launch attack
./eaphammer -i wlan0 --channel 4 --auth
wpa --ssid CorpWifi --creds
```

EAPHammer's userbase has doubled since its debut in early 2017, and the project has matured substantially to meet this demand. It is now the first rogue AP attack tool to offer out-of-the-box support for attacks against 802.11n/ac. Most of the added complexity associated with these protocols is managed automatically by EAPHammer.

We've also added some cool feature like Hashcat support, Karma, and SSID cloaking, as well as an extended UI and config management system for advanced users who require granular control over their rogue access points.

To check out the codebase, head to <https://github.com/s0lst1c3/eaphammer>

EXPL-IOT: IOT SECURITY TESTING AND EXPLOITATION FRAMEWORK

Sunday 08/12/18 from 1200-1350 at Table Two

IoT Testers- Pentesters- IoT developers- Offense- Hardware

Aseem Jakhar

Expl-iot is an open source flexible and extendable framework for IoT Security Testing and exploitation. It will provide the building block for writing exploits and other IoT security assessment test cases with ease. Exploit will support most IoT communication protocols, firmware analysis, hardware interfacing functionality and test cases that can be used from within the framework to quickly map and exploit an IoT product or IoT Infrastructure. It will help the security community in writing quick IoT test cases and exploits. The objectives of the framework are: 1. Easy of use 2. Extendable 3. Support for hardware, radio and IoT protocol analysis. We released Expl-iot ruby version in 2017. Once we started implementing hardware and radio functionality, we realized that ruby does not have much support for hardware and radio analysis which led us to deprecate it and re-write it in python to support more functionality. We are currently working on the python3 version and will release it in a month. The new beta release is envisioned to have support for UART(serial), ZigBee, BLE, MQTT, CoAP (next version will have support for JTAG, I2C and SPI) and few miscellaneous test cases.

https://bitbucket.org/aseemjakhar/exploit_framework

- ExploitIoT
- IoT Exploitation Framework
- DIVA Android (Damn Insecure and Vulnerable App)- Jugaad/Indroid
- Linux Thread injection kit for x86 and ARM
- Dexfuzzer
- Dex file format fuzzer

FIRSTORDER

Saturday 08/11/18 from 1000-1150 at Table Three

Offense

Utku Sen, Gozde Sinturk

Perimeter defenses are holding an important role in computer security. However, when we check the method of APT groups, a single spear-phishing usually enough to gain a foothold on the network. Therefore, red teams are mostly focused on "assume breach" type of scenarios. In these scenarios, testers need to use a post-exploitation framework. Besides that, testers also need to hide the server-agent communication from NIDS (Network Intrusion Detection Systems). firstorder is designed to evade Empire's C2-Agent communication from anomaly-based intrusion detection systems. It takes a traffic

capture file (pcap) of the network and tries to identify normal traffic profile. According to results, it creates an Empire HTTP listener with appropriate options.

GREYNOISE

Saturday 08/11/18 from 1200-1350 at Table Three

Defenders, blue teamers, SOC and network analysts

Andrew Morris

GreyNoise is a system that collects all of the background noise of the Internet. Using a large network of geographically and logically dispersed passive collector nodes, GreyNoise collects, labels, and analyzes all of the omnidirectional, indiscriminate Internet-wide scan and attack traffic. GreyNoise data can be used to filter pointless alerts in the SOC, identify compromised devices, pinpoint targeted reconnaissance, track emerging threats, and quantify vulnerability weaponization timelines.

<https://greynoise.io/>

GYOITHON

Sunday 08/12/18 from 1000-1150 at Table Two

Offense

Isao Takaesu, Masuya Masafumi, Toshitsugu Yoneyama

GyoiThon is a fully automated penetration testing tool against web server.

GyoiThon nondestructively identifies the software installed on web server (OS, Middleware, Framework, CMS, etc...) using multiple methods such as machine learning, Google Hacking, pattern matching. After that, GyoiThon executes valid exploits for the identified software. Finally, GyoiThon generates report of scan results. GyoiThon executes the above processing fully automatically.

GyoiThon consists of three engines:

- Software analysis engine: It identifies software based on HTTP response obtained by normal access to web server using Machine Learning base and signature base. In addition, it uses Google Hacking.
- Vulnerability determination engine: It collects vulnerability information corresponding to identified software by the software analysis engine. And, it executes an exploit corresponding to the vulnerability of the software and checks whether the software is affected by the vulnerability.

- Report generation engine: It generates a report that summarizes the risks of vulnerabilities and the countermeasure.

Traditional penetration testing tools are very inefficient because they execute all signatures. On the other hand, GyoiThon is very efficient because it executes only valid exploits for the identified software. As a result, the user's burden will be greatly reduce, and GyoiThon will greatly contribute to the security improvement of many web servers.

<https://github.com/gyoisamurai/GyoiThon>

HALCYON IDE

Saturday 08/11/18 from 1000-1150 at Table Six

Offense, Defense, AppSec, Network Security, Nmap Scanners & Developers

Sanoop Thomas

Halcyon IDE lets you quickly and easily develop Nmap scripts for performing advanced scans on applications and infrastructures with a wide range capabilities from recon to exploitation. It is the first IDE released exclusively for Nmap script development. Halcyon IDE is free and open source project (always will be) released under MIT license to provide an easier development interface for rapidly growing information security community around the world. The project was initially started as an evening free time "coffee shop" project and has taken a serious step for its developer/contributors to spend dedicated time for its improvements very actively. More information and source code: <https://halcyon-ide.org>

<https://halcyon-ide.org>

HEALTHYPI: CONNECTED HEALTH

Saturday 08/11/18 from 1400-1550 at Table Four

Hardware and biohacking

Ashwin K Whitchurch

We (at ProtoCentral) developed the HealthyPi HAT for the Raspberry Pi as a way of opening up the healthcare and open source medical to anyone. The HealthyPi is made of the same "medical-grade" components found in regular vital sign monitors, for a fraction of the cost of such system. This is our way of democratizing medical hardware to develop new areas of research.

Our objective when we began developing the HealthyPi was to make a simple vital sign monitoring system which is simple, affordable, open-source (important !) and accessible. HealthyPI is completely open-source and is our way of "hacking" patient monitoring systems by getting data that you need, in the way that you need and extending on that without getting involved in sticky proprietary NDAs and such.

Demo will allow people to come, check out and play with (and possibly hack) the HealthyPi device while getting their vital signs monitored.

<https://github.com/Protocentral/protocentral-healthy-pi-v3>

Honeycomb: An extensible honeypot framework

Saturday 08/11/18 from 1600-1750 at Table Three

Incident Responders, Security Researchers, Developers

Omer Cohen, Imri Goldberg

We present Honeycomb—A repository of honeypot services and integrations for the information security community.

Our vision: Honeycomb will be the pip or apt-get for honeypots.

While working hard to create various honeypots for several high profile vulnerabilities, we realized we were repeating some of the underlying work that's involved in creating a honeypot—a useful honeypot is easy to

deploy, configure and collects reports. We have these capabilities in Cymmetria's commercial deception product but we wanted to open source this functionality to the community so everyone could benefit from it.

Eventually came the idea for honeycomb—an extensible platform for writing honeypots which comes with a repository of useful honeypots which makes it super easy to create new honeypots. Honeycomb and the honeypot repository together form a powerful tool for security professionals looking to gain threat intelligence on the latest threats.

We are currently in the process of finalizing the release of the project and working on releasing additional plugins. Join us to learn how to utilize existing honeycomb capabilities as well as writing honeypot services and integrations on your own!

<https://github.com/Cymmetria/honeycomb>

IOC2RPZ

Saturday 08/11/18 from 1400-1550 at Table Three

Defence/Network security

Vadim Pavlov

DNS is the control plane of the Internet. Usually DNS is used for good but:

- It can be used to track users locations and their behaviour;
- Malware uses DNS to command and control, exfiltrate data or redirect traffic;
- According with 2016 Cisco annual security report, 91.3% of malware use DNS;
- Advertisements companies usually use separate and obscure domains to show ads;
- Free DNS services (e.g. 1.1.1.1, 8.8.8.8, 9.9.9.9 etc) can help you to address some concerns but you can not define your own protection settings or ad filters.

ioc2rpz is a custom DNS server which automatically converts indicators (e.g. malicious FQDNs, IPs) from various sources into RPZ feeds and automatically maintains/updates them. The feeds can be distributed to any open source and/or commercial DNS servers which support RPZ, e.g. ISC Bind, PowerDNS.

You can run your own DNS server with RPZ filtering on a router, desktop, server and even Arduino. System memory is the only limitation.

With ioc2rpz you can define your own feeds, actions and prevent undesired communications.

<https://github.com/Homas/ioc2rpz>

LHT (LOSSY HASH TABLE)

Saturday 08/11/18 from 1400-1550 at Table Six

Offense

Steve Thomas

Cracks passwords or keys from a small key space near instantly. A small key space being a few trillion (40+ bits). It costs about 3 bytes/key and usually <100ms.

The largest known deployment (made by a different less efficient program) is 160 TB. It is assumed that people are running similar ones to attack brain wallets.

<https://tobtu.com/lhtcalc.php>

LOCAL SHERIFF

Saturday 08/11/18 from 1000-1150 at Table Five

Target audience would be AppSec, Code Assessments, and privacy researchers.

Konark Modi

Think of Local sheriff as a reconnaissance tool in your browser for gathering information about what companies know about you.

While you as a user normally browse the internet it works in the background and helps you identify what sensitive information(PII—Name, Date Of Birth, Email, Passwords, Passport number, Auth tokens.) are being shared/leaked to which all third-parties and by which all websites.

The issues that Local Sheriff helps identify:

- What sensitive information with is being shared this which parties?
- What companies are behind these third parties?
- What can they doing with this information? EG: de-anonymize users on the internet, create shadow profiles.

Local Sheriff can also be used by organizations to audit:

- Which all the third-parties that are being used on their websites.
- The third-parties on the websites are implemented in a way that respect user's privacy and sensitive data is not being leaked to them.

Local Sheriff is a web-extension that can used with Chrome, Opera, Firefox.

<https://github.com/cliqz-oss/local-sheriff>

NZYME

Sunday 08/12/18 from 1000-1150 at Table One

Defense, RF, WiFi/802.11

Lennart Koopmann

Detecting attackers who use WiFi as a vector is hard because of security issues inherent in the 802.11 protocol, as well as commoditized ways of near-perfect spoofing of WiFi enabled devices. Security professionals work around this by treating WiFi traffic as insecure and encrypting data on higher layers of the protocol stack. Sophisticated attackers do not limit their efforts to jamming or tapping of wireless communication, but try to use deception techniques to trick human operators of WiFi devices into revealing secrets. The list of attacks that are possible after a user has been convinced to connect to a rogue access point that is under the attacker's control ranges from DNS spoofing to crafted captive portals that can be used for classic phishing attempts.

This is why the new nzyme release introduces its own set of WiFi deception techniques. It is turning the tables and attempts to trick attackers into attacking our own simulated, wireless infrastructure that resembles

realistic clients and access points. Together with the general collection of all 802.11 management frames already offered in the existing release, nzyme now replays all relevant communication to and from our decoy transceivers to a log management system like Graylog for analysis and alerting. This combination allows tricking attackers into revealing themselves by leaving easy to identify traces during all exploitation phases.

Applying WiFi deception to defensive perimeters gives the blue team a chance to reveal, delay, and condition attackers.<https://wtf.horse/2017/10/02/introducing-nzyme-wifi-802-11-frame-recording-and-forensics/>

GUI TOOL FOR OPENC2 COMMAND GENERATION

Sunday 08/12/18 from 1200-1350 at Table Six

Defense

Efrain Ortiz

The tool is a stand alone web self service application that graphically represents all the evolving OpenC2 commands to allow OpenC2 application developers to click and generate OpenC2 commands. The tool makes it extremely easy for even beginners to work on the creation of OpenC2 commands. The tool provides the OpenC2 command output in JSON and in curl, nodejs and python code to be easily integrate into Incident Response or Orchestration platforms.

<https://github.com/netcoredor/openc2-cmdgen>

ORTHRUS

Saturday 08/11/18 from 1000-1150 at Table Four

InfoSec

Nick Sayer

Orthrus is a small appliance that allows the user to create a cryptographically secured USB volume from two microSD cards. The data on the two cards is encrypted with AES-256 XEX mode, and all of the key material used to derive the volume key is spread between the two cards. There are no passwords to manage. If you have both cards, you have everything. If you have only one, you have half the data encrypted with a key you cannot reconstruct. This allows for “two-man control” over a dataset. Orthrus itself has no keys of its own and a volume created or written with one Orthrus can be used with any other (or on any other thing that implements the Orthrus open specification). Orthrus is open source hardware and firmware.

<https://hackaday.io/project/20772-orthrus>

PA TOOLKIT: WIRESHARK PLUGINS FOR PENTESTERS

Saturday 08/11/18 from 1600-1750 at Table Six

Defence

Nishant Sharma, Jeswin Mathai

PA Toolkit is a collection of traffic analysis plugins to extend the functionality of Wireshark from a micro-analysis tool and protocol dissector to the macro

analyzer and threat hunter. PA Toolkit contains plugins (both dissectors and taps) covering various scenarios for multiple protocols, including:

- WiFi (WiFi network summary, Detecting beacon, deauth floods, Evil twin etc.)
- VoIP (Overview of extensions, servers, Detecting invite flood, message flood, SIP auth bruteforcing, Decrypting encrypted VoIP conversation)
- HTTP (Listing all visited websites, downloaded files, streaming files, Detecting HTTP Tunnels)
- HTTPS (Listing all websites opened on HTTPS, Detecting self-signed certificates)
- ARP (MAC-IP table, Detect MAC spoofing and ARP poisoning)
- DNS (Listing DNS servers used and DNS resolution, Detecting DNS Tunnels)

The key advantage of using PA toolkit is that any user can check security related summary and detect common attacks just by running Wireshark. And, he can do this on the platform of his choice. Also, as the project is open source and written in newbie-friendly Lua language, one can easily extend existing plugins or reuse the code to write plugins of his own.

PASSIONFRUIT

Sunday 08/12/18 from 1000-1150 at Table Five

iOS reverse engineer, Mobile security research

Zhi Zhou, Yifeng Zhang

Passionfruit is a cross-platform app analyze tool for iOS. It aims to provide a powerful and user friendly gui for app pentesting and reverse engineering. In this demo we'll cover the most common tasks in iOS RE, like dumping decrypted apps from AppStore, exploring filesystem and other runtime introspections.

<https://github.com/chaitin/passionfruit>

PCILEECH

Sunday 08/12/18 from 1000-1150 at Table Four

Offense, Hardware, DFIR

Ulf Frisk, Ian Vitek

The PCILeech direct memory access attack toolkit was presented at DEF CON 24 and quickly became popular amongst red teamers and governments alike. Hardware sold out, FPGA support was introduced and devices are once again available! We will demonstrate how to take total control of still vulnerable systems via PCIe DMA code injection. Kernels will be subverted, full disk encryption defeated and shells spawned! Processes will be enumerated and their virtual memory abused—all by using affordable hardware and the open source PCILeech toolkit.

<http://github.com/ufrisk/pcileech>

-DEMO LABS-

SHOOT: AN OPEN PLATFORM FOR MANUAL SECURITY TESTERS & BUG HUNTERS

Saturday 08/11/18 from 1400-1550 at Table Two

AppSec, Mobile and Offensive security

Pavan Mohan

An open platform for bug hunters emphasizing on manual security testing.

Sh00t is a dynamic task manager to replace simple text editors or task management tools that are NOT meant for security testing provides checklists for security testing helps in reporting with custom bug templates Sh00t benefits best for pen testers, bug bounty hunters, security researchers and anybody who love bugs!

Written in Python and powered by Django web framework..

SWISSDUINO: STEALTHY USB HID NETWORKING & ATTACK

Saturday 08/11/18 from 1600-1750 at Table Four

Offense

Mike Westmacott

The Swissduino is a set of tools on an Arduino Yun that allow for the upload of binaries to target systems remotely via USB HID Keyboard, and then provide TCP connectivity between the remote attacker system and the target purely through USB HID. The demonstration shows a Metasploit Meterpreter stub being uploaded, and then actively used without triggering anti-virus (Win 7 host...).

New for 2018: (In development) Expanded toolset that allows for password extraction from login and automated installation of toolkit in Windows 10 with anti-malware/local firewall, also targeting of Linux.

TRACKERJACKER

Saturday 08/11/18 from 1200-1350 at Table One

Offensive and Defensive Wireless Hackers

Caleb Madrigal

trackerjacker is a new wifi tool that allows you to (a) see all wifi devices and which wifi networks they're connected to, along with how much data they've sent, how close by they are, etc, and (b) look for interesting traffic patterns and trigger arbitrary actions based on those patterns. The "mapping" functionality is sort of like nmap for wifi—it lists all wifi networks nearby, and under each network it lists all the clients connected to that network. The "trigger" functionality allows users to do things like "if this device sends more than 10000 bytes in 30 seconds, do something". It also includes a powerful Python plugin system that makes it simple to write plugins to do things like "if I see an Apple device with a power level greater than -40dBm, deauth it". If you want to do any sort of wifi recon/monitoring/hacking, trackerjacker will almost certainly make the job easier!

<https://github.com/calebmadrigal/trackerjacker>

WALRUS

Saturday 08/11/18 from 1400-1550 at Table Five

Offense (physical security assessors), Defense (contactless access control system users)

Daniel Underhay, Matthew Daley

Walrus is an open-source Android app for contactless card cloning devices such as the Proxmark3 and Chameleon Mini. Using a simple interface in the style of Google Pay, access control cards can be read into a wallet to be written or emulated later.

Designed for physical security assessors during red team engagements, Walrus supports basic tasks such as card reading, writing and emulation, as well as device-specific functionality such as antenna tuning and device configuration. More advanced functionality such as location tagging makes handling multiple targets easy, while bulk reading allows the stealthy capture of multiple cards while "war-walking" a target.

We'll be demoing Walrus live with multiple short- and long-range card cloning devices, as well as giving a sneak peek of future plans for the app.

<https://walrus.app/>

WHID INJECTOR: HOT TO BRING HID ATTACKS TO THE NEXT LEVEL

Saturday 08/11/18 from 1200-1350 at Table Four

Red Teams, Blue Teams and Hardware Hackers.

Luca Bongiorno

Nowadays, security threats and cyber-attacks against ICS assets, became a topic of public interest worldwide. Within this demo, will be presented how HID attacks can still be used by threat actors to compromise industrial air-gapped environments.

WHID Injector was born from the need for a cheap and dedicated hardware that could be remotely controlled in order to conduct HID attacks. WHID's core is mainly an Atmega 32u4 (commonly used in many Arduino boards) and an ESP-12s (which provides the WiFi capabilities and is commonly used in IoT projects).

Nonetheless, during the last months, a new hardware was under R&D (i.e. WHID-Elite). It replaces the Wi-Fi capabilities with a 2G baseband, which gives unlimited operational range.

This cute piece of hardware is perfect to be concealed into USB gadgets and used during engagements to get remote shell over an air-gapped environment. In practice, is the "wet dream" of any ICS Red Teamer out there.

During the demo we will see in depth how WHID and WHID-Elite were designed and their functionalities. We will also look at which tools and techniques Blue Teams can use to detect and mitigate this kind of attacks.

<https://github.com/whid-injector/WHID>

WIPI-HUNTER: IT STRIKES AGAINST ILLEGAL WIRELESS NETWORK ACTIVITIES (DETECT AND ACTIVE RESPONSE)

Saturday 08/11/18 from 1600-1750 at Table One

Offense, Defense

Besim Altinok, Mehmet Kutlay Kocer, M.Can KURNAZ

WiPi Hunter is developed for detecting illegal wireless network activities. But, it shouldn't be seen only as a piece of code. Instead, actually, it is a philosophy. You can infer from this project new wireless network illegal activity detection methods. New methods new ideas and different point of views can be obtained from this project.

Example: WiFi Pineapple attacks, Fruitywifi, mana-toolkit

WiPi-Hunter Modules:

PiSavar: Detects activities of PineAP module and starts deauthentication attack (for fake access points - WiFi Pineapple Activities Detection)

PiFinger: Searches for illegal wireless activities in networks you are connected and calculate wireless network security score (detect wifi pineapple and other fakeAPs)

PiDense: Monitor illegal wireless network activities. (Fake Access Points)

PiKarma: Detects wireless network attacks performed by KARMA module (fake AP). Starts deauthentication attack (for fake access points)

PiNokyo: If threats like wifi pineapple attacks or karma attacks are active around, users will be informed about these threats. Like proxy (New)

<https://github.com/WiPi-Hunter>



<https://infocon.org/> is a community supported archive of hacker and infosec related conferences, podcasts, documentaries, and rainbow tables.

Video is transcoded to HEVC (H.265) format to save space, put on our web server, and torrents are created to share.

Currently hosting:

151 conference, 59,520 files, 3.51 TB

50+ podcasts, 20,000+ files, 800+ Gigs

5 rainbow tables, 19,869 files, 10.3 TB

Want in on the file action? Check out:

- The con media server, <https://dc26-media.defcon.org/>

- The Data Duplication Village for 6TB HDD duplication

- <https://infocon.org/> for the latest files and torrents

See something we are not hosting? Tell us about it so we can add it to the archive. email info@infocon.org or on twitter DM @infoconorg

New for 2018, infocon.org is reachable as a v3 Tor onion at:
<http://w27irt6ldaydjoacyovepuzlethuoyapazhbot6tljuywy52emetn7qd.onion/>

-VENDORS-

BREAKPOINT BOOKS

<http://breakpointbooks.com/>



Stop by and browse the wide selection of security-related books on display this weekend. The latest and greatest books available in the industry also include books authored by Def Con presenters. Check out the wide selection of games available – strategy, card, dice, and deck-building. Buy a game and start playing today.

CAPITOL TECHNOLOGY UNIVERSITY

<https://www.capttechu.edu/>



Capitol Technology University, located in Laurel Maryland, offers degrees in engineering, computer science, cybersecurity, and business. Offering online certificates, bachelor's and master's degrees, which includes a master's in astronautical engineering.

As well as doctoral programs in cybersecurity and management and decision sciences. Capitol is regionally accredited by Middle States Association of Colleges.

EFF

<https://www.eff.org/>



The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We defend free speech on the Internet,

fight illegal surveillance, support freedom-enhancing technologies, promote the rights of digital innovators, and work to ensure that the rights and freedoms we enjoy are enhanced, rather than eroded, as our use of technology grows. Stop by our table to find out more, pick up some gear, or even support EFF as an official member.

GHETTO GEEKS



Well we're back at it again, and have been working hard all year to bring you the freshest awesome that we can. If you have been to DEF CON, layerone,

toorcon, phreaknic, or other conferences we have been at, you definitely know what so of shenanigans we are up to. If you have never seen us, feel free to come by and take a look at what we have to offer.

Always fun, always contemporary, GhettoGeeks has some for the tech enthusiast (or if you prefer, hacker)

GUNNAR

<https://gunnar.com/>



GUNNAR Optiks is the only patented computer eyewear recommended by doctors to protect and enhance your vision. Our premium computer eyewear defends eyes from the effects of digital eye strain which can include; dry eyes, headaches, blurry vision, eye fatigue, altered Circadian Rhythms, and insomnia. End the pain of DIGITAL EYE STRAIN.

HACKERBOXES

www.hackerboxes.com



HackerBoxes is the subscription box service for DIY electronics and hardware hacking. Each monthly HackerBox includes a carefully curated collection of projects, components,

modules, tools, supplies, and exclusive items. HackerBox Hackers are electronics hobbyists, makers, hardware hackers, and computer enthusiasts. Many connect through social media channels to create a community of experience, support, and ideas. Let's see what you make with your HackerBoxes.

HACKER WAREHOUSE

<http://hackerwarehouse.com/>



HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why

we carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

HACKERS FOR CHARITY

<http://www.hackersforcharity.org/>



Hackers for Charity is a non-profit organization that leverages the skills of technologists. We solve

-PURVEYORS OF FINE HACKER-RELATED MERCHANDISE-

technology challenges for various non-profits and provide equipment, job training and computer education to the world's poorest citizens.

HAK5

<https://www.hak5.org/>



Complete your Hacking Arsenal with tools from Hak5 - makers of the infamous WiFi Pineapple, USB Rubber Ducky, and newly released LAN Turtle. The Hak5

crew, including hosts Darren Kitchen, Shannon Morse and Patrick Norton, are VENDING ALL THE THINGS and celebrating 10 year of Hak5! Come say EHLO and check out our sweet new tactical hacking gear! Everything from WiFi Hot-Spot Honey-Pots to Keystroke Injection tools, Software Defined Radios and Covert LAN Hijackers are available at the Hak5 booth.

HARDWARE ZOO

Did someone say badges? Check out our unique blinky badges and add-ons before they're all gone!

HEALTHY MENTALS

<https://healthymentals.com/>



Healthy Mentals offers nootropics and other supplements.

HUMAN RIGHTS FOUNDATION

<https://www.hrf.org/>



Human Rights Foundation (HRF) is a nonpartisan nonprofit organization that promotes and protects human rights globally, with

a focus on closed societies. HRF unites people in the common cause of defending human rights and promoting liberal democracy. Its mission is to ensure that freedom is both preserved and promoted around the world.

KEYPORT

<https://www.mykeyport.com/>



Keyport@ combines keys, pocket tools, & smart tech into one everyday multi-tool. This year we are bringing our

brand new modular product line including the Keyport Slide 3.0 & Keyport Pivot (holds your existing keys), along with our new tech & tool modules which includes a Pocketknife, Bluetooth Locator, and Mini-Flashlight. Sign up for our new Maker Program and design/hack/build you're own compatible Keyport modules. Don't forget to bring your keys to the vendor area!

NO STARCH PRESS

<https://www.nostarch.com/>



Thanks to you, we've been publishing books for hackers since 1994. Our titles have personality, our authors are passionate, and our books tackle topics that people care about. We read and edit everything we publish—titles like Gray Hat C#, Hacking: The Art of Exploitation, Automate the Boring Stuff with Python,

Python Crash Course, The Hardware Hacker, and more. This year we're excited to release the PoC|GTFO bible; complete with a leatherette cover, ribbon bookmark, and gilded pages. It's packed with missives from your favorite hackers. Everything in our booth is at least 30% off and all print purchases include DRM-free ebooks. We've got new swag and early access print editions of forthcoming titles like Serious Cryptography, Attacking Network Protocols, and Rootkits and Bootkits.

OWASP



OWASP is the thriving global community that drives visibility and evolution in the safety and security of the world's software. We are run by rough consensus & running code. Our community supports hackers, developers, and defenders in the security industry.

NUAND

<https://www.nuand.com/>



Nuand develops Software Defined Radio (SDR) platforms for students, hobbyists, and professionals. Their main offering, the bladeRF,

-VENDORS-

is a versatile USB 3.0 device that provides a 300 MHz to 3.8 GHz tuning range, full duplex operation, 12-bit samples at up to 40 MSPS, and an instantaneous bandwidth up to 28 MHz. This device has found a home in application domains including GSM and LTE base stations, digital television, GPS simulation, medical imaging research, and wireless security. Check out their booth to see demos and learn more!

RAPID7

<https://www.rapid7.com/>



Rapid7 cybersecurity analytics software and services reduce threat exposure and detect compromise for 4,150 organizations, including 34% of the Fortune 1000. From the endpoint to cloud, we provide comprehensive real-time data collection, advanced correlation, and unique insight into attacker techniques to fix critical vulnerabilities, stop attacks, and advance security programs.

SCAM STUFF

<http://scamstuff.com>



Scam Stuff is gear for the modern rogue: magic tricks, lockpicking, puzzle boxes, clever novelty items, spy gear, and more! If it's designed to get you ahead, you'll find it here.

SECURITY SNOBS

<https://securitysnobs.com/>



Security Snobs offers High Security Mechanical Locks and Physical Security Products including door locks, padlocks, cutaways, security devices, and more. We feature the latest in security items including top brands like Abloy, BiLock, EVVA, KeyPort, Mobeye, Anchor Las, and Sargent and Greenleaf. Visit <https://SecuritySnobs.com> for our complete range of products. Stop by to see the new and coming soon products in high security and con specials!

SEREPICK

<http://www.serepick.com/>



With the largest selection of lock picks, covert entry and SERE tools available at DEF CON it's guaranteed we will have gear you have not seen before. New tools and classics will be on display and available for sale in a hands on environment. Our Product range covers Custom

Titanium toolsets, Entry Tools, Practice locks, Bypass tools, Urban Escape & Evasion hardware and items that until recently were sales restricted. SPARROWS LOCK PICKS and TOOLS will be displaying a full range of gear including their newly released Core Shims., Sandman and Lock Outs. The WOLF will also be available to the public for the first time in limited quantities. All products will be demonstrated at various times and can be personally tested for use and efficacy.

SHADOWVEX INDUSTRIES

<http://store.shadowvexindustries.com/>



Shadowvex Industries (SVX) - more than 20 years of pouring blood, sweat & gears into hacker-relevant,

limited edition clothing, DJ mixes, stickers, buttons, art prints and more. Miss DJ Jackalope, aka DEFCON's resident DJ mixtress, has been teaming up with us for more than a decade with her own DJ mixes and awesome swag. Follow the music in the vending area to find our booth! If you want to bring home your piece of DEFCON history, you need to get here early - our year-specific designs are only available @DEFCON and only while supplies last!



SIMPLE WIFI

<https://www.simplewifi.com/>



For PenTesting and unwired Internet Security

Specialists: Wireless, WiFi antennas, cables, connectors, USB and Ethernet wireless high power cards and devices, other interesting goodies to be seen only at the table! And new design T-shirts.

TOOOL

<http://toool.us/>



The Open Organisation Of Lockpickers is back as always, offering a wide selection of tasty lock goodies for both

the novice and master lockpicker! A variety of commercial picks, handmade picks, custom designs, practice locks, handcuffs, cutaways, and other neat tools will be available for your perusing and enjoyment! Stop by our table for interactive demos of this fine lockpicking gear or just to pick up a T-shirt and show your support for locksport.

All sales exclusively benefit TOOOL, a 501(c)(3) non-profit organization. You can purchase picks from many fine vendors, but ours is the only table where you know that 100% of your money goes directly back to the hacker community.

-PURVEYORS OF FINE HACKER-RELATED MERCHANDISE-

UAT

<http://www.uat.edu/>



The University of Advancing Technology (UAT) is a private university located in Tempe, Arizona, offering academic degrees focused on new and emerging technology disciplines. UAT offers a robust suite of regionally accredited graduate and undergraduate courses

ranging from Computer Science and Information Security to Gaming and New Media. UAT has been designated as a Center for Academic Excellence in Information Systems Security Education by the US National Security Agency. Programs are available online and on-campus.

360 UNICORN TEAM

<http://unicorn.360.cn/>



360 Security Research Innovation Alliance consists of many teams, UnicornTeam, RocTeam and PegasusTeam are among them, each team boasts many brilliant researchers in their corresponding field of focus.

UnicornTeam is focusing on wireless security they assess the security of anything that uses radio technologies, from small things like RFID, NFC and WSN to big things like GPS, UAV, Smart Cars, Telecom and SATCOM. They have presented their researches at premier security conferences like Blackhat, DEFCON, HITB, CanSecWest, RuxCon, POC, SyScan360 etc.

RocTeam is focusing on hardware security research and the R&D of hardware that can be used for defensive and offensive purposes, they built many hardware security gadgets.

PegasusTeam is focusing on wireless intrusion prevention, wireless threat sensing and wireless penetration test. They have designed and built 'MianYangQiang' to demonstrate the threats of public WIFI, wireless honeypot, wireless intrusion prevention system '360TianXun' which have been widely deployed city wide and in enterprises.

WISP

<https://www.wisporg.com/>



Women in Security and Privacy (WISP) is a fiscally sponsored non-profit project of Community Initiatives (501(c)(3)). WISP advances women to lead the future of security and privacy. We believe that empowerment requires the inclusion of all women,

with expertise in both security and privacy. Our work includes education, mentoring & networking, career advancement, leadership, and research. To learn more, visit us at <https://www.wisporg.com>.

ATTIFY

CLOUDFLARE

DARKNET LLC

FREENODE



HACKER STICKERS



KINKAYO

MALICIOUS LIFE PODCAST

SECURITY WEEKLY

SEWASHREE

THE CALYX INSTITUTE



TENCENT

FIRESIDE HAX

FRIDAY

OH NOES! A ROLE PLAYING INCIDENT RESPONSE GAME

20:00-22:00 in Roman Chillout

Bruce Potter

DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

20:00-22:00 in Octavius 9

Christian "quaddi" Dameff MD & Jeff "r3plicant" Tully MD

DISRUPTING THE DIGITAL DYSTOPIA OR WHAT THE HELL IS HAPPENING IN COMPUTER LAW

20:00-22:00 in Octavius 13

Nathan White & Nate Cardozo

SATURDAY

EFF FIRESIDE HAX (AKA ASK THE EFF)

20:00-22:00 in Roman Chillout

BEYOND THE LULZ: BLACK-HAT TROLLING, WHITE-HAT TROLLING, AND HACKING THE ATTENTION LANDSCAPE

20:00-22:00 in Octavius 9

Matt Goerzen & Jeanna Matthews

PRIVACY IS EQUALITY: AND IT'S FAR FROM DEAD

20:00-22:00 in Octavius 13

Sarah St.Vincent

CONTEST CLOSING CEREMONIES

WANNA KNOW WHO IS THE BEST AT FINDING RANDOM STUFF AROUND LAS VEGAS DURING DEF CON? CURIOUS WHO IS THE BEST AT SOCIAL ENGINEERING SOMEONE INTO GIVING UP PRIVILEGED PERSONAL OR COMPANY DATA? WHAT ABOUT THE BEST TEAM TO BE HARASSED, FED LOTS OF BOOZE AND STILL ABLE TO WRITE AND COMPILE EPIC CODE?

COME JOIN US AS WE ANNOUNCE THE WINNERS OF THE DEF CON 25 CONTESTS AT OUR CONTESTS CLOSING CEREMONIES, FROM 14:00 - 15:30PM ON THE STAGE ON THE MAIN CONTEST FLOOR!

BLACK BADGE WINNERS WILL BE ANNOUNCED DURING THE MAIN CLOSING CEREMONIES AT 16:30PM IN TRACK 2!

-THURSDAY-

101 Track	
10:00	ThinSIM-based Attacks on Mobile Money Systems Rowan Phipps
11:00	Pwning "the toughest target": the exploit chain of winning the largest bug bounty in the history of ASR program Guang Gong
12:00	Ring 0/2 Rootkits: bypassing defenses Alexandre Borges
13:00	A Journey Into Hexagon: Dissecting a Qualcomm Baseband Seamus Burke
14:00	Wagging The Tail - Covert Passive Surveillance And How To Make Their Life Difficult Si & Agent X
15:00	Building the Hacker Tracker Whitney Champion & Seth Law
15:30	DC 101 PANEL (Until 16:45)

-FRIDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	Synfuzz: Building a Grammar Based Re-targetable Test Generation Framework Joe Rozner	Badge/DT Welcome	De-anonymizing Programmers from Source Code and Binaries Rachel Greenstadt & Dr. Aylin Caliskan	Securing our Nation's Election Infrastructure Jeanette Manfra
10:30				Please do not Duplicate: Attacking the Knox Box and other keyed alike systems m010ch_
11:00	An Attacker Looks at Docker: Approaching Multi-Container Applications Wesley McGrew	NSA Talks Cybersecurity Rob Joyce	One-liners to Rule Them All Egypt	Lora Smart Water Meter Security Analysis Yingtao Zeng
12:00	It's Assembler, Jim, but not as we know it: (ab) using binaries from embedded devices for fun and profit Morgan "Indrora" Gangwere	Vulnerable Out of the Box: An Evaluation of Android Carrier Devices Ryan Johnson	Breaking Paser Logic: Take Your Path Normalization Off and Pop 0days Out! Orange Tsai	Who Controls the Controllers - Hacking Crestron IoT Automation Systems Ricky "HeadlessZeke" Lawshae
13:00	Dissecting the Teddy Ruxpin: Reverse Engineering the Smart Bear Zenofex	Compromising online accounts by cracking voicemail systems Martin Vigo	Finding Xori: Malware Analysis Triage with Automated Disassembly Amanda Rousseau & Rich Seymour	One-Click to OWA William Martin
13:30	You can run, but you can't hide. Reverse engineering using X-Ray. George Tarnovsky	Dragnet - Your Social Engineering Sidekick Truman Kain	Attacking the Brain: Customize Evil Protocol to Pwn an SDN Controller Feng Xiao	Fasten your seatbelts: We are escaping iOS 11 sandbox! Min Zheng
14:00	UEFI exploitation for the masses Mickey Shkatov	GOD MODE UNLOCKED - hardware backdoors in x86 CPUs Christopher Domas	4G - Who is paying your cellular phone bill? Dr. Silke Holtmanns & Isha Singh	Revolting Radios Michael Ossmann & Dominic Spill
15:00	Weaponizing Unicode: Homographs Beyond IDNs The Tarquin	Bypassing Port-Security In 2018: Defeating MacSEC and 802.1x-2010 Gabriel Ryan	Playback: a TLS 1.3 story Alfonso Garcia Alguacil & Alejo Murillo	Privacy infrastructure, challenges and opportunities yawnbox
16:00	Automated Discovery of Deserialization Gadget Chains Ian Haken	Your Peripheral Has Planted Malware - An Exploit of NXP SOC's Vulnerability Yuwei Zheng	Practical & Improved Wifi MitM with Mana Singe	Your Voice is My Passport _delta_zero
17:00	Your Bank's Digital Side Door Steven Danneman	I'll See Your Missile and Raise You A MIRV: An overview of the Genesis Scripting Engine Alex Levinson	Panel - The L0pht Testimony, 20 Years Later (and Other Things You Were Afraid to Ask)	Reverse Engineering, hacking documentary series Michael Lee Nirenberg

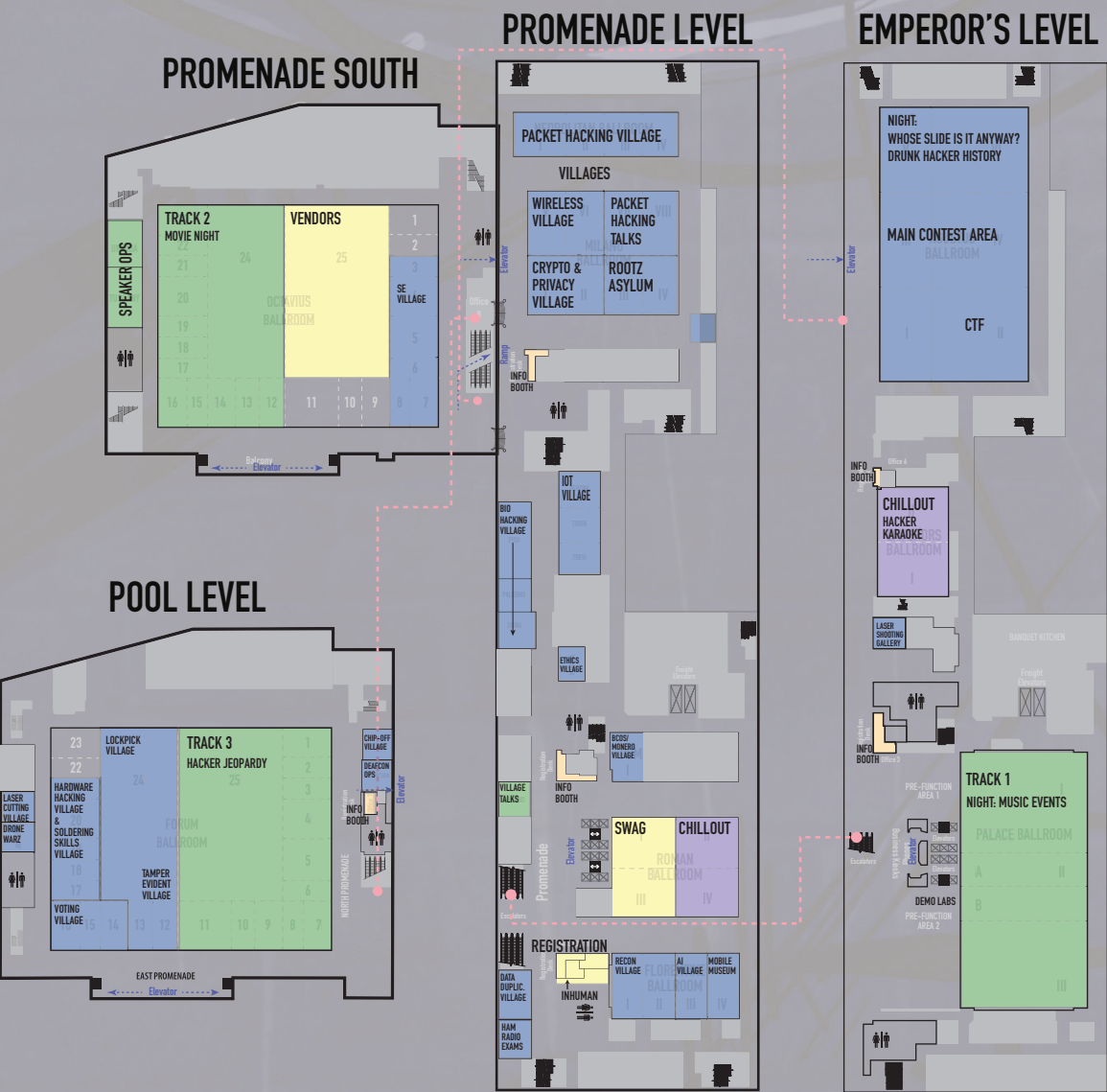
-SATURDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	Through the Eyes of the Attacker: Designing Embedded Systems Exploits for Industrial Control Systems Marina Krotofil	It WISN't me, attacking industrial wireless mesh networks Erwin Paternotte	You're just complaining because you're guilty: A Guide for Citizens and Hackers to Adversarial Testing of Software Used In the Criminal Justice System Jeanna Matthews	You may have paid more than you imagine - Replay Attacks on Ethereum Smart Contracts Zhenxuan Bai
11:00	Hacking PLCs and Causing Havoc on Critical Infrastructures Thiago Alves	Exploiting Active Directory Administrator Insecurities Sean Metcalf	Compression Oracle Attacks on VPN Networks Nafeez	Jailbreaking the 3DS through 7 years of hardening smea
12:00	TBA	Tineola: Taking a Bite Out of Enterprise Blockchain Stark Riedesel	You'd better secure your BLE devices or we'll kick your butts! Damien "virtualabs" Cauquil	Ridealong Adventures - Critical Issues with Police Body Cameras Josh Mitchell
13:00	One Step Ahead of Cheaters -- Instrumenting Android Emulators Nevermoe	In Soviet Russia Smart-card Hacks You Eric Sesterhenn	Reaping and breaking keys at scale: when crypto meets big data Yolan Romailier	Looking for the perfect signature: an automatic YARA rules generation algorithm in the AI-era Andrea Marcelli
13:30	House of Roman - a "leakless" heap fengshui to achieve RCE on PIE Binaries Sanat Sharma	The ring 0 façade: awakening the processor's inner demons Christopher Domas	Detecting Blue Team Research Through Targeted Ads 0x200b	Infecting The Embedded Supply Chain Zach
14:00	Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices Dennis Giese	SMBetray - Backdooring and breaking signatures William Martin	Digital Leviathan: a comprehensive list of Nation-State Big Brothers (from huge to little ones) Eduardo Izycki	Playing Malware Injection with Exploit thoughts Sheng-Hao Ma
14:30			Sex Work After SESTA/FOSTA Maggie Mayhem	Fire & Ice: Making and Breaking macOS Firewalls Patrick Wardle
15:00	Project Interceptor: avoiding counter-drone systems with nanodrones David Melendez Cano	All your math are belong to us sghtoma	Reverse Engineering Windows Defender's Emulator Alexei Bulazel	Booby Trapping Boxes Ladar Levison
16:00	Outsmarting the Smart City Daniel "unicornFurnace" Crowley	80 to 0 in under 5 seconds: Falsifying a medical patient's vitals Douglas McKee	All your family secrets belong to us - Worrisome security issues in tracker apps Dr. Siegfried Rasthofer	Inside the Fake Science Factory Dr. Isabella Stein
17:00	CLOSED	The Road to Resilience: How Real Hacking Redeems this Damnable Profession Richard Thieme	Relocation Bonus: Attacking the Windows Loader Makes Analysts Switch Careers Nick Cano	

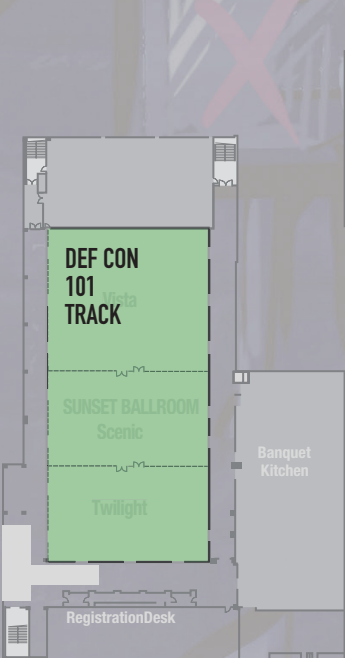
-SUNDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	The Mouse is Mightier than the Sword Patrick Wardle	Rock appround the clock: Tracking malware developers by Android "AAPT" timezone disclosure bug. Sheila A. Berta & Sergio De Los Santos	Defending the 2018 Midterm Elections from Foreign Adversaries Joshua M Franklin	For the Love of Money: Finding and exploiting vulnerabilities in mobile point of sales systems Leigh-Anne Galloway
11:00	Searching for the Light: Adventures with OpticSpy Joe Grand (Kingpin)	Breaking Extreme Networks WingOS: How to own millions of devices running on Aircrafts, Government, Smart cities and more. Josep Pi Rodriguez	Politics and the Surveillance State. The story of a young politician's successful efforts to fight surveillance and pass the nation's strongest privacy bills. Daniel Zolnikov	Demystifying MS17-010: Reverse Engineering the ETERNAL Exploits zerosum0x0
12:00	Breaking Smart Speakers: We are Listening to You. Wu HuiYu	Last mile authentication problem: Exploiting the missing link in end-to-end secure communication Thanh Bui	Attacking the macOS Kernel Graphics Driver Yu Wang	Designing and Applying Extensible RF Fuzzing Tools to Expose PHY Layer Vulnerabilities Matt Knight
13:00	Trouble in the tubes: How internet routing security breaks down and how you can do it at home Lane Broadbent	Man-In-The-Disk Slava Makkaveev	Micro-Renovator: Bringing Processor Firmware up to Code Matt King	barcOwned - Popping shells with your cereal box Michael West
13:30		Asura: A huge PCAP file analyzer for anomaly packets detection using massive multithreading Ruo Ando	Lost and Found Certificates: dealing with residual certificates for pre-owned domains Ian Foster	Edge Side Include Injection: Abusing Caching Servers into SSRF and Transparent Session Hijacking Idionmarcil
14:00	Betrayed by the keyboard: How what you type can give you away Matt Wixey	Your Watch Can Watch You! Gear Up for the Broken Privilege Pitfalls in the Samsung Gear Smartwatch Dongsung Kim	Hacking BLE Bicycle Locks for Fun and a Small Profit Vincent Tan Kwang Yue	One bite and all your dreams will come true: Analyzing and Attacking Apple Kernel Drivers Xiaolong Bai & Min Zheng
15:00	Closed	Panel DCGroups	What the Fax!? Yaniv Balmas	Fuzzing Malware For Fun & Profit. Applying Coverage-guided Fuzzing to Find and Exploit Bugs in Modern Malware Maksim Shudrak
16:30	Closed	Closing Ceremonies	Closed	Closed
17:00				

CAESAR'S PALACE CONFERENCE CENTER



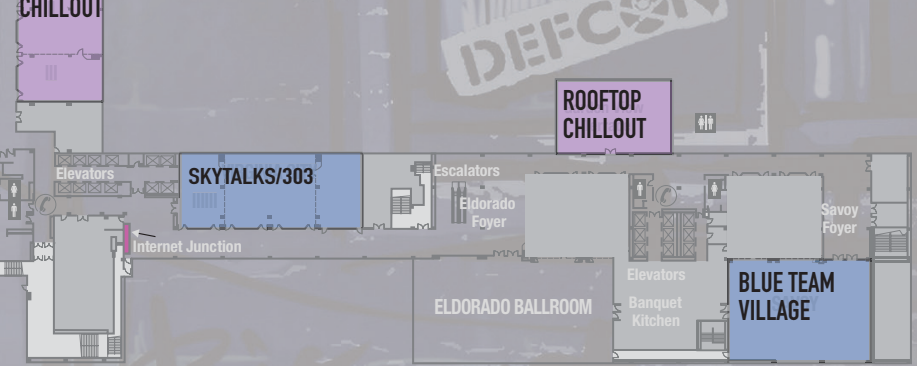
FLAMINGO LAS VEGAS



EXECUTIVE CONFERENCE CENTER LOWER LEVEL



CORPORATE CONVENTION CENTER THIRD FLOOR



-SHOUT OUTS-

The Dark Tangent would like to thank Jeff, Nikita, Sleestak, Neil, Charel, Will, and Janet for putting up with me year round, through the thick and thin of starting DEF CON China, and the questions sent at all hours.

I would especially like to thank everyone who attended DEF CON 26 and for believing in our community. It is your enthusiasm, energy, and creativity that fuels us and keeps DEF CON on the edge. I would also like to thank the 1,600+ people, from the Goons to the hotel staff and speakers to the contest organizers, who made this all possible by building the content, experiences, and memories for us all to enjoy!

A&E:

ChrisAM would like to thank everyone responsible for this year's entertainment & decor: Krisz Klink, Great Scott, Zziks, dead, CTRL, stitch, davesbase, Zebbler Studios, Mobius, and SomaFM.

CONTENT:

Nikita would like to thank the DEF CON 26 Reviewers for their help in selecting the content for two DEF CON's this year, DC26 and DC China. We are very thankful for the dedication and support we showed each other as a team. We have banded together four days of content in the form of presentations, workshops, firesides. Thank you! CFP Board: Claviger, The Dark Tangent, Dead Addict, High Wizard, Jericho, Malware Unicorn, MavAntagonist, Medic, Nikita, PWCrack, Roamer, Security Barbie, Shaggy, Suggy, Tuna, Vyrus, Wiseacre, Yan, ZFasel, Zoz. Special Reviewers: Andrea Matwyshyn, Chris Sistrunk, Grifter, snow, Wonk. Workshop Reviewers: Ash, Beaker, CyberSulu, Da Kahuna, HighWiz, Munin, SinderzNAsheS, Tottenkoph, Wiseacre

CONTESTS & EVENTS:

Grifter would like to thank every Goon on the Contests Team. Many thanks to panadero, stumper, phorkus, phartacus, saltr, heisenberg, Apexxor, Secove, ArmyTra1n3d, gomer, rcu83d, Zero3, lol_newb, fr33jack, Gmark, Trevor.

DCGROUPS:

Thank you to April, Brent, Casey, Darington, Jayson E Street, Neil/Drifter, s0Ups, and byt3boy.

DESIGN:

Neil would like to thank Nikita, Sleestak, and Mar, for all the creative help behind the scenes pre-con. Thanks to Posterboy for the awesome signage and putting up with all the last minute stuff. Shout out to Supafraud for some sweet videos. Cathy at Olympus for having my back. And finally, thanks to my new on-site deployment team Medic, Xaphan, and friends, and to all of you for making it worth doing!

DISPATCH:

RF and Ahab would like to thank AsmodianX, Taclane, and Voltage Spike for helping to lead the Dispatch team, and wish to thank the rest of the Dispatch Staff for always going above and beyond: BonBon, Fosgood, L0G1C, Dimes, Rixon, w00k, dlI3ma, Archangel, dirtclod and miggles.

INFO:

InfoBooth: Mello and LittleBruzer would like to thank all the InfoBooth goons for bad information and sending humans in the wrong direction. We would also like to thank the humans for the interesting questions they asked.

NOC:

Welcome to DEF CON 26! As usual efffn and DEF CON would like to thank all the hard work and planning of our rockstar NOC team, they put a lot of work in so you guys can enjoy many aspects of the con. As usual, by the time you're reading this, months of planning happened and crazy few days of execution on site have been lived to cover everything we do for the con, especially now with multiple venues. We strive to attend requests from mostly all departments of the con, from vendors, speakers, press, contests, DC TV, workshops, infobooth and so on. mac, #sparky, CRV, c0mmiebstnd, c7five, Jon2, deadication, musa, wish and john sacrificed a great portion of their DEF CON experience to making sure everything breaks the right way (so we know how to fix it ASAP). If you happen to run into any of them, please make sure you thank them and possibly buy them a beverage. The entire NOC team would like to thank the Caesar's IT and Encore teams for the tireless support in making it all a bit easier for us.

PARTY:

The DEF CON Party GOONS (Beef "xistence" Supreme, Delchi, Apok, Pyr0, and our "Noons") would like to thanks the hacker community, 303, Security Tribe, the Skytalks staff, 1057, The Dark Tangent, ALL DEF CON GOONS (past, present, and future). Respect, memory, and love to those who are no longer with us. Xistence would like to give a special thanks to Delchi for his work leading up to con and the party organizers, without them we would be rather bored since there wouldn't be anything fun to do at night. Thanks be to Sk0d , who sits at the side of Odin and watches over our analysts. In memoriam recolitur The Nightstalker (cDc/NSF) , The Dorsai Embassy NYC Hackerspace. Shai Dorsai!

PHOTO:

Photo Goons would like to thank: ASTCell, Cannibal, Loather, noise, mrB0t and InfoSystir.

PRODUCTION:

Charel in Hotel and Production would like to thank: C0njur3r, kampf, 4C3, Betsy, Ira, Killerspud, V-Gorilla, jup1t3r, supertechguy, L34N, metacortex, skyria, Dumby, Prod_Goon_22, HiveQueen, and sn1ck3r5. Call us when you need us!

PRESS:

A Big Thank You to all the press who not only cover the DEF CON community, but are part of it, as well as all the Press Goons: Alan, Alex, Jeff, Heather, Landyn, Lin, Linda, Mel, Melanie, Mike, Monika, Nicole, and Sylvia!

QM:

"There is a part of DEF CON that will be forever England" - at least I think that's the quote... QM Stores is a magical place of pelican cases and barcodes, British Water (or Juniper Mallets), the gentle sounds of Goons at work - the odd grunt here, the whizz of the coffee grinder there, the chirrup of a printer churning out a sign-in sheet, and last but not least, the heady aroma of sweaty Goon arse crack, namely those of: ETA, Waz, Zac, Buttersnatcher, Sunsh1ne, Multigrain, Youngblood, Red Ace, Lord Drimacus, Noise, mrb0t, The Saint, Big Eezee, Seven, Ge0, shell_e, Cell Wizard and Major Malfunction. BTW (an acronym, not a handle!), RijilV, Slacker, RageQuit, Uncle IRA, Josh and Minor, we miss you!!! May Bob bless us, and all who flail in us!

REGISTRATION:

The awesome folks on the human and inhuman reg teams; f1dget and apebit, taking charge; all those who always come through in the clutch but won't be mentioned here; TW; Tyler and Matt; SOC, QM, Swag, and Info Booth; the line wranglers; anyone anywhere who spends their con moving heavy stuff from one place to another; and the attendees, as always, for their patience.

SOC:

Cjunky and tacitus would like to thank every past, present, and future SOC Goon who have built this team and family that we are proud to be a part of, including this year's team: AdaZebra, Alpha Kilo, Amber, Angie, heartbreaker, Arc, arcon, Ast0r, Atriyen, b3l, BeaMeR, Bogaaron, Br1ck, Carric, cheronobyl, Chosen1, CHRIS, cRusad3r, cymike, Dallas, Darkwolf, deelo, dr.kaos, DrFed, duckie, echosixx, Emex, Faz, Fox, g33kspeed, gadams, George, Glasswalk3r, GodFix, hamster, Hanzo, iCandy, iole, iv4t, Jbone, JohnD, Judo, Junior, KRS, kruger, Labrat, Lordy, M0rph1x, matrix, mauvehed, MIM, Mr. M, n1cfury, n3x7, NextInLine, nohackme, Nothingness, onetwo, Oselot, P33v3, ph3r, Phat_Hobbit, Plasma, polish_dave, prec0re, Priest, Rabbit, RadioActive, Randy_Wat?, Raven, Red, rotor_rabbit, SAGE, Salem, Sam, sl3dge, Slick, Siviak, SomeNinja, Sonicos, sp00ns, Spedione, stan, stealth,

Sumdunce, Synn, TBD, TieFighter, timball, WarFlower, wham, WhiteB0rd, wilnix, Wreaktifier, YoursTruly, ZephhrFish, zerofux, and Zulu. Pax Per Imperium.

SPEAKER OPS:

Proctor would like to thank the Speaker Operations staff for another year of great service to DEF CON its speakers. These goons are pwcrack, Pasties, Crash, Pardus, Mnky, CLI, Jur1st, Scout, Goeke, Bitmonk, phliKtd, Bushy, Vaedron, idontdrivecars, K-hole, StOnehouse, notkevin, Flattire, nerfherder, Jutral, Milhouse, g8, DaKahuna, Gattaca, Mubix, Surreal Killer, RoundRiver, Jinx and AMFYOO!

SWAG:

Secret would like to thank all the Swag goons: Lisa33, Daria, rudy, 10rn4, spiggy, pelican, Themikeconnor, Csp3r, Daedala, Skyfall, gingerjet, gLoBuS, H4zy, endsu, Serenity, BearClaw, Magnar, Alligatro, Heal, Brizan, furysama, Loak, PeeJ, Zubion, Alex, D20OwlBear, TheViking, Trevot, webjedi, and Mr.Katt for all their hard work and all the other departments who make DEF CON possible!

VILLAGES:

Zantdoit would like to thank Br00zer for being crazy enough to join me on the quest for standing up a new section and the trials of growing that section all in one year. A huge shoutout to Amlazar, Runner-up, Zant's daughter, and Hony for all their help in keeping things organized. Villages have grown a lot this year, which would not be possible without the help of all the Goons who help keep it running. So to the Village Goons... Thanks to those who are returning and welcome to all the new ones joining the team. Zantdoit and Br00zer also want to thank all the Village leads and organizers for everything they do to make all these great villages possible.

WORKSHOPS:

Tottenkoph thanks all of those who worked to review the workshop proposals this year, Neil and Nikita for all of the hard work and help they do, her amazing team of goons (SinderzNAsheS, beaker, cybersulu, flipper, Joel & Jenn Cardella, Jay Radcliffe, mav, binarybuddha, fallible, gillis, Rand0h, and lawyerliz), and the teams/ leads that help to support us before/during the show.

VENDORS:

Will & Janet from Vendors would like to thank Lsly, pinball, Redbeard, Rob Collins and Wad for all their hard work, and all the other departments for making DEF CON an incredible community based Hacker convention!

