

# DEFENSE





# Welcome to



This year's theme is the "Promise of Technology" done in a Retro Futurism style. After last year's "1983," the year before Orwell, we wanted to provide an alternative vision of the future. A different path. One not so dark and depressing but full of positive potential?

Exhibit A: Crystal Electronic Badges that can be worn on your wrist.

What is the promise of technology? What could be its higher purpose? Technology should be a reflection of our society, not just of a few mega companies.

I suggest "Promise Tech" would strengthen those things that help us do good, and weaken the things that enable us to do bad. The business model would not be surveillance capitalism and captive marketing but instead reflect the real costs of technology. It is opt-in, not opt-out.

Transparent, audit-able, and reproducible algorithms would be the norm, not the exception. Prediction algorithms would help enlighten us, not take us down dark rabbit holes and divide us. Your devices would be repairable, recyclable, even.. upgrade-able. More John Perry Barlow and less Mark Zuckerberg.

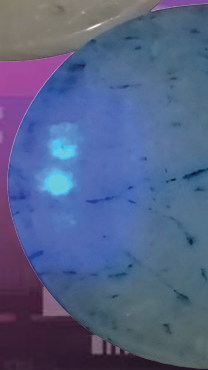
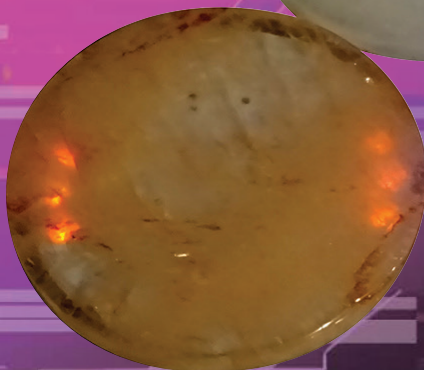
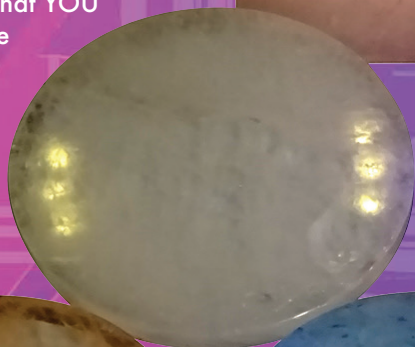
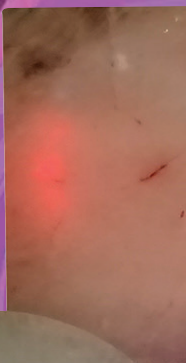
If we are to achieve any bit of it we will need to be fully involved in not only the design and deployment decisions, but also the social policy debates. No matter what we will need to hack the shit out of it to make sure the security promises are real.

We are spanning four hotels this year, with more space for workshops, villages, and even our own night club at Planet Hollywood. This is all part of my master plan to help you make friends by creating opportunities through badge to badge interaction, village hands on exploration, and evening lounge talks. Yes DEF CON is larger, but we work hard to make it feel smaller.

DEF CON remains supported by attendees buying stuff like badges and shirts, and has no sponsors. This is by design and I believe it helps keep us focused on the community instead of the corporations.

While it takes almost 1,200 Goons, speakers, organizers of villages, contests, events and artists to operate the con, the key is that YOU make it happen. We have set the scene, now it is up to you to make the con yours.

-The Dark Tangent



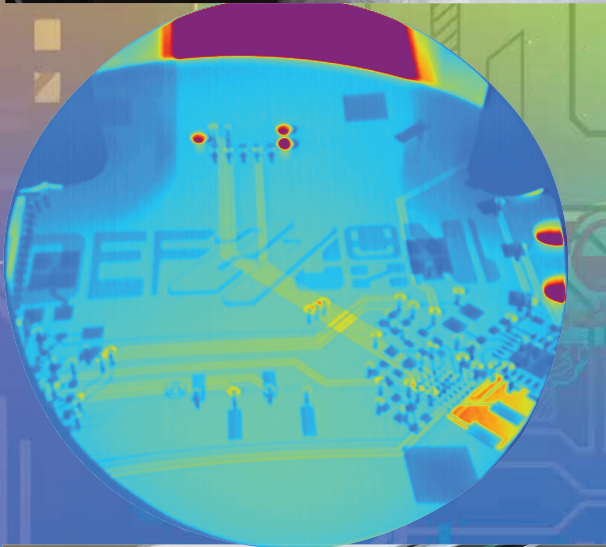


# THE BADGE

Imagine if technology had kept its promise to help us achieve more, to be better people, and grow our community in a positive direction. Instead of a world where technology is used primarily for manipulation, tracking, and control, imagine if it was used only for building, sharing, and empowering without pretense, fine print, or financial interest.

This year's badge is a manifestation of Technology's Promise. Deceptively simple, yet deviously complex, it contains a quest for you to experience all that DEF CON has to offer. As you complete certain tasks around the event, your badge will advance through different stages. Complete all the tasks and unlock your true potential!

It's been an honor to create this badge for you after so many years of "retirement" and I'm excited to see it in action. Enjoy DEF CON and good luck on your quest!



JOE GRAND  
AKA  
\$KINGPIN\$

- Joe Grand aka Kingpin





# NETWORK AND DCTV

## NETWORK INSTRUCTIONS

The DEF CON NOC delivers the best zero-trust network access throughout the different hotel properties using all of the blockchainz, ML and AI (ai ais).

If you want to get online using the Wi-Fiz, 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, wildest-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 (still), never forget we're talking about the Wi-Fiz: where radio wavez make packets fly and digital voodoo makes the communications secure, dodging the haxored deepwebz and those pineapples along the way.

We do 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.

By configuring 802.1X 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 no bueno.

Be an advocate of cyber common sense (™), and 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. Make something up, be creative, and funny. Like a clown.

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 NOC updates visit <https://www.defconnetworking.org> and also follow us on the twitterz @DEFCON\_NOC, for shenanigans go to zero-trust.af

## DCTV RETURNS!

DEF CON TV is back this year. Our goal is to provide content to seven hotels this year. For more info on what hotels and channels are up and running please visit <https://DCTV.defcon.org/>

## THE DEF CON MEDIA SERVER IS BACK AGAIN!

<https://10.0.0.16/> or

<https://dc27-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 dc27-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/"
```



# CODE OF CONDUCT/RESOURCES

## 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 for the second year in a row we have 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) 222-0934.

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+.



A vibrant, comic-style illustration of the word 'GOON' in large, bold, black letters with yellow outlines. The letters are set against a background of a city skyline at night, with yellow and orange light flares. A blue, mechanical-looking arm with a yellow eye-like sensor is positioned in front of the letters. The overall style is energetic and futuristic.

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:

DEF CON 27 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 27 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 be 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 27 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](mailto: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  
 **GOON**





# CHILLOUT AT NAPOLEON'S

**WE HAVE NAPOLEON'S ALL TO OURSELVES!**

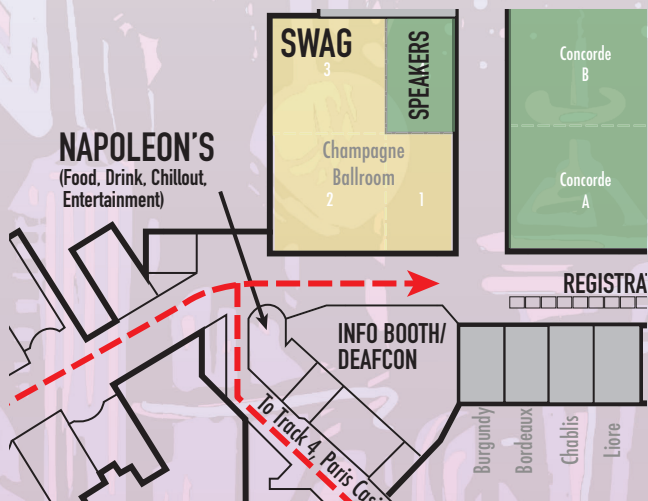
**CHILLOUT AND LIVE MUSIC, STAY OR GO FOOD AND DRINK OPTIONS, AND A GREAT PLACE TO PAUSE AND REFLECT!**

## FRIDAY LIVE MUSIC!

21:00 - 22:00 - Steph Infection  
 22:00 - 23:00 - s7a73farm  
 23:00 - 00:00 - Acid-T a.k.a dj sm0ke  
 00:00 - 01:00 - Wil Austin  
 01:00 - 02:00 - ASHSLAY

## SATURDAY LIVE MUSIC!

21:00 - 22:00 - DJ Th@d  
 22:00 - 23:00 - Azuki  
 23:00 - 00:00 - Magik Plan  
 00:00 - 01:00 - E.ghtB.t  
 01:00 - 02:00 - Yurk



Located in Paris next to Con  
 entrance  
 Napoleon's Operating hours as  
 Chillout are:  
 Friday 11am - 2am  
 Satrday 11am - 2am  
 Sunday 11am-3pm



# MUSIC

## PLANET HOLLYWOOD - GALLERY NIGHTCLUB

### THURSDAY

2100 TINEH NIMJEH  
2200 ARCHWISP  
2300 CTRL  
0000 RODMAN  
0100 SEEKER

### FRIDAY

TERRESTRIAL ACCESS NETWORK  
ICETRE NORMAL  
MISS JACKALOPE  
DJ ST3RLING  
DJ%27

### SATURDAY

KAMPF  
ICETRE NORMAL  
SCOTCHANDBUBBLES  
ACID-T AKA DJSMOKE  
CLOCKWORK ECHO

### FRIDAY

2100 E.GHTB.T  
2200 AMPLITUDE PROBLEM FT YTCRACKER  
2300 TBA  
0000 TBA  
0100 MAGIK PLAN

### SATURDAY

SKITTISH & BUS  
MISS JACKALOPE  
ZEBBLER ENCANTI EXPERIENCE  
TBA  
NINJULA

## PARIS - VENDOME A,B,C





# PARTIES & MEETUPS

## DEF CON LADIES MEETUP

Meetup on Thursday at 17:00 - 19:00,  
located in Sin City at Planet Hollywood

Women & nonbinary people come to meet, get to know each other & do fun girl/hacking/geeky stuff together! RSVP (not required) <https://www.meetup.com/HackerFoodies/events/262691815/>

PS: We have a discord for the Women attending DEF CON or HackerSummerCamp in general. If you want an invite send a DM to @sylv3on\_ @nemessisc or @CircuitSwan

## VETCON II

Party on Friday at 19:30 - 02:00,  
located in Rivoli A at Paris

Back again! VETCON is 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.

Twitter: @VetConActual

## SECKC THE WORLD AGAIN

Party on Friday at 21:00 - 02:00,  
located in London Club/Night Club at Planet Hollywood

SeckKC is back. But this time, they're shooting for the stars! Roll up on your favorite thoroughbred and make sure to bring your intergalactic western gear. Outlaws and sheriffs alike are welcome!

This party is happening in a beautiful old cabaret club that will be getting the SeckKC mojo treatment ;) And music will be provided by none other than Keith Myers, Archwisp, and Professor SI! Come join us for dancing, games, and other various shenanigans. The party starts at 10:00 and goes until the last hacker leaves!

<https://seckc.org/>

## SKYTALKS

Party on Friday at 19:30 - 02:00,  
located in Concorde A at Paris

Friday night will be a place for con-goers to meet and greet the speakers from Skytalks. We'll also have DJs and potentially have live music too.

<https://skytalks.info>

## BLANKETFORT CON

Party on Friday at 19:30 - 02:00,  
located in Concorde B at Paris

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

<https://twitter.com/blanketfortcon?lang=en>

## DIVERSITY PARTY

Party on Friday at 19:30 - 02:00,  
located in Concorde B at Paris

hacker outreach" event

Follow T:@DefConOwasp for updates

August 9th @8PM

Concorde B in Paris

Swing by between 8-10PM+ on the 9th of August to connect with others.

Come and meet cool groups and crews, we encourage you to come and take a space at the event : )

Come hang and meet others, make new friends, see what others are working on : )

Learn about & meet organizations that are working to bring empowerment and inclusion to the hacker community.

We are next to Blanket Fort Con: )

## HACKER KARAOKE

Party on Friday & Saturday at 19:30 - 02:00,  
located in Concorde C at Paris

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.

## BADASS/CYBER SEXURITY

Meetup on Friday at 15:00 - 18:00,  
located in Sin City at Planet Hollywood





An open discussion on agency, sexuality, and harassment/abuse in tech. What can we do, as a community, to make spaces safer for everyone? How can we encourage more sex positive discussions? Let's talk about it.

oosball table! Jam out to special guest DJ's while taking another swipe at that high score on your favorite classic video games. No quarters required! Sponsored by: SCYTHE, GRIMM, Dragos, Bugcrowd, and ICS Village



# DEF CON MOVIE NIGHT

27

FILM	LOGAN'S RUN	STAR TREK:TMP	GATTACA	DEMOLITION MAN
				
TIME	FRIDAY 8PM	FRIDAY 10PM	SATURDAY 8PM	SATURDAY 10PM
LOCATION	PLANET HOLLYWOOD - MELROSE FOUR			
SYNOPSIS	THE WORLD IS CLEAN AND BRIGHT, EVERYONE IS PRETTY, BUT HANG ON TO 29 AS LONG AS YOU CAN.	OG STATUS. EVEN WHEN THE EFFECTS WERE RUDIMENTARY AND THE LINE READINGS... WERE...PECULIAR.. STAR TREK SAW A FUTURE WHERE MANKIND TRANSCENDS SCARCITY AND WAR AND NEEDS TO VENTURE OUTWARD TO FIND SOCIAL STRIFE TO MIDDLE IN. ALSO, LCARS.	SET IN AN UNCOMFORTABLY NEARBY FUTURE, GATTACA ASKS SOME TOUGH, CONTEMPORARY QUESTIONS. WHAT HAPPENS WHEN YOU HAVE THE TOOLS TO 'PERFECT' A CHILD? WHAT HAPPENS WHEN ONLY SOME PEOPLE CAN ACCESS SAID TOOLS? IS THERE AN INCREDIBLY PAINFUL WAY TO LENGTHEN ONE'S CALVES?	AFTER THE DUST SETTLES ON THE FRANCHISE WARS, SOCAL FALLS INTO A RIGOROUSLY ENFORCED SYSTEM OF PUBLIC SAFETY AND CIVIL ORDER. WHICH WORKS GREAT, UNTIL SOMEONE UNFREEZES THE 90S (PLAYED BY WESLEY SNIPES), A TOXIN FOR WHICH THE FUTURE HAS NO ANTIDOTE.
MISSION STATEMENT	SCIENCE FICTION LOVES AN URBAN DYSTOPIA. EXPOSED REBAR, OMINOUS CLOUDS AND A THICK LAYER OF PERMA-GRIME - YOU KNOW THE DRILL.  IN ORDER TO CONNECT TO THE THEME OF DEF CON 27, HOWEVER, WE NEEDED TO FIND FILMS WITH A DIFFERENT VIBE. WE LOOKED FOR MOVIES WITH A VISION OF THE FUTURE WHERE TECH CREATES HARMONY AND COMFORT INSTEAD OF PARANOIA - AT LEAST IN ACT ONE. OBVIOUSLY, THINGS MAY GO PRETTY SIDEWAYS FROM THERE.			
X-HOUR FILM CONTEST	SATURDAY'S MOVIE NIGHT WILL ALSO SHOW THE ENTRIES TO THE TD FRANCIS X-HOUR FILMMAKING CONTEST. COMPETING TEAMS WILL MAKE A SHORT FILM DURING DEF CON 27, IN A "48 HOUR" FILM CONTEST FORMAT.			



# PARTIES & MEETUPS

## 303

Party on Saturday at 19:30 - 02:00,  
located in Rivoli B at Paris

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!

## ARCADE PARTY

Party on Saturday at 19:30 - 02:00,  
located in Rivoli A at Paris

Relive once again the experience of the arcade at DEF CON. From classics to a custom built 16 player foosball table! Jam out to special guest DJ's while taking another swipe at that high score on your favorite classic video games. No quarters required! Sponsored by: SCYTHE, GRIMM, Dragos, Bugcrowd, and ICS Village

## GOTHCON

Party on Saturday at 19:30 - 02:00,  
located in Front room Gallery Night Club at Planet Hollywood

Back for our second year, in the gorgeous Front room of the Gallery Bar in Planet Hollywood on Saturday August 10th. GOTHCON (or #dcgothcon) is a collection of goths, goth-adjacent, friends of goths, and others who just wanted to hang out in their favorite outfits and listen to some goth-of-center music. It's a fun space for \*everyone\* to make friends and have fun during DEF CON. We encourage people to dress up however they want, to come with open minds, and to not be a jerk. Everyone is welcome!

<https://www.gofundme.com/f/gothcon-defcon-party> Twitter: @dcgothcon

## HACKER FLAIRGROUNDS

Meetup on Saturday at 19:30 - 02:00,  
located in London Club at Planet Hollywood

Flaming badge builder or just badge curious Hacker Flairgrounds is the ultimate gathering of hackers and blinking LEDs in Vegas."

This is the Meetup destination for badge collectors, designers, and prototypers that you have been waiting for! A social environment to show off your custom badges, discuss projects to make your 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.

## LAWYERS MEET

Meetup on Friday at 18:00 - 20:00,  
located in Napoleons Corner Bar at Paris

If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join Jeff McNamara at 18:00 on Friday, August 9th, for a friendly get-together, drinks, and conversation. Location: Inside the Napoleons Bar just outside of the Paris Speaking Tracks.

## FRIENDS OF BILL W

Meeting, Thurs-Sat at 12:00 and 17:00, Sun at 12:00

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is SANTA MONICA 4 in Planet Hollywood.

## UNOFFICIAL DEF CON 27 MEETUP FOR /R/DEFCON

Meetup, Friday at 18:00 in Le Bar Du Sport (Next to Paris Sports Book)

Alrighty friends, it's time to start planning out our DC27 gathering! I know, I know... It took me way longer to get this posted than it usually does, but the important part is that it's finally here and we can have some spend some time together in person!! I'm super pumped as the meetup has been gaining traction each year and I'm looking forward to seeing how many people we can get together to chat, relax, and share a drink or two (if that's your jam).

As usual, it's difficult to find a time that everybody is able to make it to, but Friday nights typically seem to be the best in terms of conflicts. However, If y'all think we can find a better time, let me know!!

### General Information

I can get to the bar a little early and gather some tables in a corner, and if anybody wants to help me out there will be a beer or two (and maybe a high-five, if you are lucky) in it for you!

I am so excited to see everybody again! See you at camp!

# VILLAGES

## AI VILLAGE

Friday: 10:00 - 18:30, Saturday: 10:00 - 18:30, Sunday: 10:00 - 14:00

Location: Bally's, Skyview 3

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 with help in the evenings after the tals. Or come checkout some deepfakes and AI generated art and listen to some of the latest research into security with ML. 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 with help in the evenings after the tals. Or come checkout some deepfakes and AI generated art and listen to some of the latest research into security with ML.

## APPSEC VILLAGE

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

Location: Flamingo, Mesquite BR

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

Village Schedule: <https://www.appsecvillage.com/agenda>

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

Twitter: [https://twitter.com/AppSec\\_Village](https://twitter.com/AppSec_Village)

## AVIATION VILLAGE

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

Location: Bally's, Event Center

Aviation is a cornerstone of our global infrastructure and economy. While passenger safety is at an all time high, the increasing adoption of connected technologies exposes aircraft, airports, and the interdependent aviation ecosystem to new types of risks. The consequences of cybersecurity failure

can impact human life and public safety; a crisis of confidence in the trustworthiness of air travel can undermine economic and (inter)national security.

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

The Aviation Village will create a first-of-its-kind platform to bridge the gap between the security research community and the aviation community. The Aviation Village will do this by:

Building connections, trust, and understanding among all Village participants.

Developing aviation security skills among DEF CON attendees through workshops and hands-on activities.

Promoting constructive dialog through talks and interaction.

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

Village Schedule: <https://aviationvillage.org/village-schedule/>

Website: [aviationvillage.org](https://aviationvillage.org)

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

## BCOS BLOCK CHAIN VILLAGE

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

Location: Flamingo, Laughlin III

After making a solid debut at DEF CON 26, BCOS Village is back again as Blockchain Village. Along side Monero group we had a great event comprising of 26 talks, Panel Discussions and back2back multiple contests, diving deep in to various security and privacy aspects of Blockchain & Cryptocurrency.

As we are seeing Blockchain getting more main streamed, and the huge support we got from the community at DEF CON, this year we are planning to bring in more variety, wider range of topics, contests, research papers and more representatives from around the world.

Right from Governance, Election management, Education credentials and certification management, Logistics, supply chain to property records management, every field where blockchain is being implemented, will be included at Blockchain Village.

Not to forget various cryptocurrency, Exchange houses, Academia and also the IT-Giants which provide one click deployment for Blockchains,



all are eager to extend their support and share their security & privacy practices with the community at DEF CON, will be integral part.

As innovations in Blockchain Technology are making new breakthroughs every day, we have a lot to catchup on security front. We have lot to research, break, demonstrate, discover and educate to make the Blockchains more robust and better.

So get involved with us as we bring you brand new & awesome talks, contests, workshops, discussions and celebrations with Blockchain Village at DEF CON 27.

Website: [blockchainvillage.net](http://blockchainvillage.net)

Twitter: @bcosvillage

## BIO HACKING VILLAGE

Thursday: 10:00 - 18:00/19:00, Friday: 10:00 - 20:00, Saturday: 10:00 - 20:00, Sunday: 10:00 - 14:00

Location: Planet Hollywood, Melrose 1-3

The Biohacking Village celebrates global health ingenuity arising from maker communities with the dynamic perspective of emerging biology, technology, and human-enhancement. Whether your interest lies in security, technology, engineering, devices, or fabrication, BHV donors can be assured they are reaching an audience of unapologetically enthusiastic innovators.

The BioHacking Village will bring together attendees, along with featured inventors, world-class makers, cybersecurity researchers, self-made entrepreneurs & workshop experts from around the world, to create real solutions for some of humanity's most pressing challenges and opportunities in the areas of health, education, security, and more.

You will be immersed in the biomaker community on a local grassroots level that allows you to build relationships with makers, hackers, and others. We encourage the development of an ongoing dialogue and the forging of lasting relationships.

We will have three rooms dedicated to the bio ecosystem:

**Speakers Room:** Presentations on cool new tech, hacks, or discoveries

**Medical Devices:** Hospital setup with various medical devices for your hacking pleasure

**Hands-on Lab:** Work on experiments and get your hands a little dirty

## BIOHACKING VILLAGE WORKSHOP

Thursday, Friday, Saturday, Sunday

Location: Planet Hollywood, Melrose 1

## BIOHACKING VILLAGE: HANDS ON LAB

Friday: 1000-1900, Saturday: 1000-1900, Sunday: 1000-1400

Location: Planet Hollywood, Melrose 1

Attendees will be actively working on various projects/experiments by watching and interacting with researchers in a hands-on environment. Practical skills are the key to success and some scientific jargon used in labs will be clarified. These courses are not a comprehensive biology course, so do not expect too much theoretical knowledge. This course will provide you with relevant information in real-time during the hands-on exercise. By the end you will be able to successfully perform their own experiments.

Village Schedule: <https://www.villageb.io/learning-lab>

## BIOHACKING VILLAGE: SPEAKERS

Friday: 1000-1800, Saturday: 1000-1900, Sunday: 1000-1430

Location: Planet Hollywood, Melrose 2

Like all hackers, we are looking to subvert the dominant paradigm of life itself. How can we use technology to enhance our raw abilities, specific skills, overall health, or well-being? How can we usher in an age where we not only fix what is broken, but we make our world and ourselves, better? Just as the early computer hackers challenged the status quo to introduce us to the real possibilities of computing, we dare to sit on the cutting edge to create our own miracles from the raw materials of biotechnology.

The Biohacking Village (BHV) is a collaborative movement focused on breakthrough information security, DIY biology, human augmentation, medical technology, and related communities in the biotech ecosystem. Our village will excite, elucidate, enlighten, and engage participants in the technical, mechanical, procedural, and human side of biohacking. There are multiple instances of DIYBio overcoming conventional science which we support and present through a compendium of talks and demonstrations. We invite you to come and expand your understanding of what it means to be a biohacker!

Village Schedule: <https://www.villageb.io/speaker-hub>

## BIOHACKING VILLAGE: DEVICES

Friday: 1000-1800, Saturday: 1000-1900, Sunday: 1000-1200

Location: Planet Hollywood, Melrose 3

The Biohacking Village, in collaboration with I Am The Cavalry, runs a Medical Device Lab at DEF CON to improve trust and trustworthiness of the public health system. The Lab is a high-trust, high-collaboration environment where security researchers can learn and build their skills alongside patients, medical device makers, hospitals, the FDA, and others. We

# VILLAGES

welcome participants who will act in good faith, in the best interest of patients, when researching, disclosing, and addressing security issues.

Village Schedule: <https://www.villageb.io/device-lab>

Website: [villageb.io](http://villageb.io)

Twitter: @DC\_BHV

## BLUE TEAM VILLAGE

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

Location: Flamingo, Savoy BR

Welcome to the other side of the hacking mirror. Blue Team Village (our friends just call us BTv) is both a place and a community built for and by defenders. It's a place to gather, talk, share, and learn from each other about the latest tools, technologies, and tactics that our community can use to detect attackers and prevent them from achieving their goals.

BTv packs more fun and learning into three days than any defender can possibly fit in. If you like to compete in CTFs, we have two: This year we are again hosting the uniquely blue Network Defense OpenSOC CTF, and we've also added the equally creative BiaSciLab's Bia Hak Lab CTF. Maybe you just want to hang out in the Village with like minded defenders. Maybe you prefer to learn from over a dozen defender focused talks, or get hands-on training in a half dozen defender workshops. Maybe you'll want to buy the insanely cool BTv badge that gives you access to our underground networking, threat intel meet-up, and party at Blue Team Village After Dark (BTvAD). We're not gonna say if there will be live entertainment, but who knows? We guess you'll have to see that for yourself. Oh... Did we mention that the BTv badge is a hackable platform based on the Pi Zero W and that it will have WiFi AP mode, badge to badge comms, and various honeypots?

BTv promises to be an all out firehose of Blue Team learning, sharing, and fun for the defenders that build stuff, defend stuff, and just make it generally hard for attackers. Come celebrate the other side of the hacking mirror with us. We'll keep a blue light on for you!

Village Schedule: [www.blueteamvillage.org](http://www.blueteamvillage.org)

Website: [www.blueteamvillage.org](http://www.blueteamvillage.org)

Twitter: [www.twitter.com/blueteamvillage](https://www.twitter.com/blueteamvillage)

Other: [www.reddit.com/user/blueteamvillage](https://www.reddit.com/user/blueteamvillage)

## CAR HACKING VILLAGE

Friday: 10:00 - 18:00, Saturday: 10:00 - 18:00, Sunday: 10:30 - 12:30

Location: Bally's, Event Center

Learn, hack, play. The Car Hacking Village is an open, collaborative space to hack actual vehicles that you don't have to worry about breaking! Don't have tools? We'll loan you some. Never connected to a car? We'll show you how. Don't know where the controllers are? We'll show you how to take it apart.

Additionally we'll host a Donkey Car race.

Check out our web site for up to date info.

Want to race? Check out of full car simulator(s).

Want to learn more about automotive hacking

and cyber security? Check out our talks.

Want to hack mobility scooters? Yes! We'll do that to.

Also, check out the CHV CTF.

Check out [carhackingvillage.com](http://carhackingvillage.com) for the latest information.

Village Schedule: [carhackingvillage.com/dc27](https://carhackingvillage.com/dc27)

Website: [carhackingvillage.com](http://carhackingvillage.com)

Twitter: @carhackvillage

## CLOUD VILLAGE

Friday: 14:00 - 18:00, Saturday: 10:00 - 18:00, Sunday: 10:00 - 13:00

Location: Flamingo, Reno I

Cloud Village is an open space to meet folks interested in offensive and defensive aspects of cloud security.

Village Schedule: <https://cloud-village.org/#timelines>

Website: <https://cloud-village.org/>

## CRYPTO & PRIVACY VILLAGE

Friday: 10:00 - 19:00, Saturday: 10:00 - 19:00, Sunday: 10:00 - 13:30

Location: Planet Hollywood, Celebrity I & 2

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 workshops and talks on a wide range of crypto and privacy topics from experts. We'll also have an intro to crypto talk for beginners, some crypto-related games, and puzzles.

Village Schedule: <https://cryptovillage.org/dc27/>

Website: <https://cryptovillage.org>

Twitter: @Cryptovillage

## DATA DUPLICATION VILLAGE

Thursday: 16:00 - 19:00, Friday: 10:00 - 17:00, Saturday: 10:00 - 17:00, Sunday: 10:00 - 11:00

Location: Bally's, Event Center Office

Yes, the Data Duplication Village is back and better than ever for DC 27! If you're looking for something to fill up all your unused storage, may I recommend a nice hash table or two with a side of all of the DEF CON talks and everything else on infocon.org? It's all part of our "free-to-you" service of simply handing you terabytes of useful data.

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

### HOW IT WORKS

DEF CON provides a core set of drive duplicators and data content options. We accept 6TB drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in 6TB SATA3 blank drives and check them in early to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO!



## WHAT YOU GET

We're still working out the details but this is what was provided for DC26...

- 6TB drive 1-3: All past hacking convention videos that DT could find, built on last years collection and always adding more for your data consuming appetite.
- 6TB drive 2-3: freerainbowtables.com hash tables (1-2)
- 6TB drive 3-3: GSM A5/1 hash tables plus remaining freerainbowtables.com data (2-2)

## THAT'S ALL?

But wait - there's more! We had a great round of inaugural talks last year and are looking to improve on a good thing! It's submission dependent, of course, but we pick the best so check dcddv.org for the schedule of talks. This year, our stretch goal is to add pick-and-pull data stores to the DDV. Come see if we actually made it happen!

All the details can be found on dcddv.org or in the DC Forum thread and you are encouraged to ask any questions you have there.

Welcome to Vegas!

Village Schedule: <https://dcddv.org/dc27-schedule>

Website: <https://dcddv.org>

Twitter: @DDV\_DC

## DEF CON HARDWARE HACKING VILLAGE

Friday: 10:00 - 19:00, Saturday: 10:00 - 19:00, Sunday: 10:00 - 13:00  
Location: Bally's, Event Center

Join us for another DEF CON adventure! Another year, another set of hardware hacking tricks and tips to show off! We are again sharing a (very) large space with the Soldering Skills Village and are colocated with other villages that love hardware. This puts all of your hardware hacking/making resources in one place. For more details on hours and other events, see dchhv.org

Village Schedule: <https://dchhv.org/dc27-schedule.html>

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

Twitter: [https://twitter.com/dc\\_hhv](https://twitter.com/dc_hhv)

## DRONEWARZ VILLAGE

Friday: 10:00 - 18:00, Saturday: 10:00 - 18:00, Sunday: 10:00 - 13:00  
Location: Bally's, Event Center

### FIGHT in FLIGHT

choose a side ...

A Drone is an Unmanned Ariel Vehicle (UAV)/ Unmanned Aircraft System (UAS) capable of autonomous flight and DroneWarz allows you to adapt these aircraft to fight in flight. Get ready to see something straight out of a sci-fi movie. Introducing.... DroneWarz!

Our big event is our CTF (Capture the Flag) Drone Cage Match held annually at DEF CON. This is a CTF like no other. The DroneWarz CTF offers unique flags that bridge all villages of DEF CON into a

single game. You will need some serious skill to win in this highly competitive arena. Enter at your own risk and be ready to make friends because the audience may also choose sides and join the game!

In addition to our CTF, DroneWarz also offers drone hacking training, unique games, hacking objectives, contests, and challenges which are designed to harness innovation and have fun with emerging UAV technologies. Join us and engage our drone testing benches with several challenges that will allow you to explore drones in ways that will inspire and ignite an industry in flight! Get ready to Fight in Flight! Join DroneWarz today!

Flight | Fight

Website: <https://dronewarz.org>

## ETHICS VILLAGE

Friday: 12:00 - 18:00, Saturday: 12:00 - 18:00, Sunday: 11:00 - 14:00  
Location: Flamingo, Reno II

The DEF CON Ethics Village is focused on fostering a discussion about ethics in the security domain. 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. 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. The Ethics Village is sponsored by DC 217 an interest group for computer security topics.

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

## HACK THE SEA VILLAGE

Friday: 10:00 - 18:00, Saturday: 10:00 - 18:00, Sunday: 10:00 - 13:00  
Location: Bally's, Event Center

In 1995, when the fictitious Dade Murphy and his friends stopped oil tankers from being capsized by a virus in the movie "Hackers", "digital piracy" was just a euphemism for sharing music with disregard for the DMCA. By the 2000s, frequent DEF CON speaker Moxie Marlinspike showed one could have a passion for both the sea and hacking.

Today? To quote The Conscience of a Hacker "This is our world now... the world of the electron and the switch, the beauty of the baud." Modern ships are increasingly automated industrial control systems (ICS) and Operational Technology (OT), networked via satellite and cellular broadband communications, to make them a floating extension of the Internet of Things (IoT).

The organizer's of Hack The Sea 2019 believe it is

# VILLAGES

possible to “To build a future that doesn’t limit our love of modern technology and socialization at the expense of freedom...”. Seasteading, for example, may hold the key to realizing many of same ideals as crypto-anarchy. The sea offers a place, which like the internet, could let us build a future for humanity beyond national boundaries. Threats to that future will include not only threats from the surveillance state to privacy, but also threats from pirates to human life and vital infrastructure. But we’re hackers, we’ll figure it out.

Join us at the DEF CON 27, for Hack The Sea 2019, as the voyage begins.

Village Schedule: [www.hackthesea.org](http://www.hackthesea.org)

Website: [https://twitter.com/hack\\_the\\_sea](https://twitter.com/hack_the_sea)

Twitter: <https://www.instagram.com/hackthesea/>

## HAM VILLAGE

Thursday: 15:00 - 18:00, Friday: 10:00 - 18:00, Saturday: 10:00 - 18:00, Sunday: 10:00 - 14:00

Location: Flamingo, Virginia City II

Wait, isn’t ham radio what my grandpa does in his basement with that old tube radio? Well, yes, that is ham radio too, but it’s more than that.

Village Schedule: <https://www.hamvillage.org>

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

## ICS VILLAGE

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

Location: Bally’s, Event Center

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

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

Why. High profile Industrial Controls 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 these systems and how to better prepare and respond to the changing threat landscape.

Exhibits. Interactive simulated ICS environments, such as Hack the Plan(e)t and Howdy Neighbor, provide safe yet realistic examples to preserve safe, secure, and reliable operations. We bring real components such as Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), Remote Telemetry Units (RTU), actuators, to simulate a realistic environment throughout different industrial sectors. Visitors can connect their laptops to assess these ICS devices with common security scanners, network sniffers to sniff the industrial traffic, and more!

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

## INTERNET OF THINGS VILLAGE

Friday: 09:30 - 18:30, Saturday: 09:30 - 18:30, Sunday: 09:30 - 13:00

Location: Flamingo, Eldorado Ballroom

Organized by security consulting and research firm Independent Security Evaluators (“ISE”), IoT Village advocates for advancing security in the Internet of Things (IoT) industry. IoT Village hosts talks by expert security researchers, interactive hacking labs, and competitive IoT hacking contests. Over the years IoT Village has served as a platform to showcase and uncover more than 300 new vulnerabilities, giving attendees and sponsors the opportunity to learn about the most innovative techniques to both hack and secure IoT. A DEF CON 24 Black Badge ctf, players compete against one another by exploiting off-the-shelf IoT devices. These 15+ devices all have known vulnerabilities, but to successfully exploit these devices requires lateral thinking, knowledge of networking, and competency in exploit development. CTFs are a great experience to learn more about security and test your skills, so join up in a team (or even by yourself) and compete for fun and prizes! Exploit as many as you can over the weekend and the top three teams will be rewarded.

Village Schedule: [https://www.iotvillage.org/#dc27\\_schedule](https://www.iotvillage.org/#dc27_schedule)

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

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

Other: <https://twitter.com/ISEsecurity>

## LOCK BYPASS VILLAGE

Friday: 11:00 - 17:00, Saturday: 10:00 - 19:00, Sunday: 10:00 - 13:00

Location: Flamingo, Carson City I

Lock Bypass Village explores all the ways you can hack physical security that don’t involve lockpicking. Try your hand at door hardware bypass techniques, disabling alarm systems and cameras, and applying a hacker mindset to secured physical spaces. Come learn advanced methods for physical red-teaming in today’s world - or just learn the ropes (and we mean that literally, too)!

Just about every type of locking hardware has a bypass vulnerability, which we have here for you to learn and try out. If you want to up the stakes, try disabling alarms and security systems by attacking the sensors, communication lines and everything in between.

We’ll run a few village talks to teach the basics, and to cover exploits we can’t easily reproduce at DEF CON -

- Come out to “Lock Bypass 101” to do a whirlwind tour of the exploits available, and how to use them in context.
- Learn about alarm and response timing, avoiding and interacting with security, and other practical considerations for redteaming by attending “So You Want to Rob a Bank: Overt Ops Timing & Practise”.
- Finally, see what you are capable of doing by climbing, jumping, squeezing and pulling in “The Human Body’s Promise: How Your



Bare Hands can Defeat Physical Security”.

Finally, we'll have all of the blue team's tools for you to try as well - for every exploit you learn, we'll show you the patch. We'll also demonstrate integrated approaches to secure facilities by considering security as an interconnected system rather than a bunch of individual boxes to be checked. Finally, we're happy to discuss at length how to apply this methodology to whatever specific facility or operation you have in mind - it is our job, after all!

Village Schedule: <http://lbv.ggrsecurity.com/#sched>

Website: <http://lbv.ggrsecurity.com>

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

## LOCK PICK VILLAGE

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

Location: Bally's, Platinum BR

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: [twitter: https://twitter.com/toool](https://twitter.com/toool)

## MONERO VILLAGE

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

Location: Bally's, Skyview 4

The Monero project is a privacy ecosystem which consists of several cryptocurrency relevant projects and workgroups. The village presents technology serving privacy-conscious novice and advanced cryptocurrency users, inviting participation in a well-equipped and comfortable environment. 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.

Village Schedule: <https://www.monerovillage.org/dc27/schedule/>

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

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

Other: <irc://chat.freenode.net/#monero-defcon/>

## PACKET HACKING VILLAGE

Friday: 10:00 - 18:00, Saturday: 09:00 - 18:00, Sunday: 10:00 - 14:30

Location: Bally's, Skyview 5-6, 1-2 (Indigo Tower, 26th Floor)

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. 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. WoSDJCo 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 its run.

Village Schedule: <https://wallofsheep.com/pages/dc27>

Website: <https://wallofsheep.com>

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

## ROOTZ ASYLUM

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

Location: Planet Hollywood, The Studio

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/2019-schedule>

Website: [www.r00tz.org](http://www.r00tz.org)

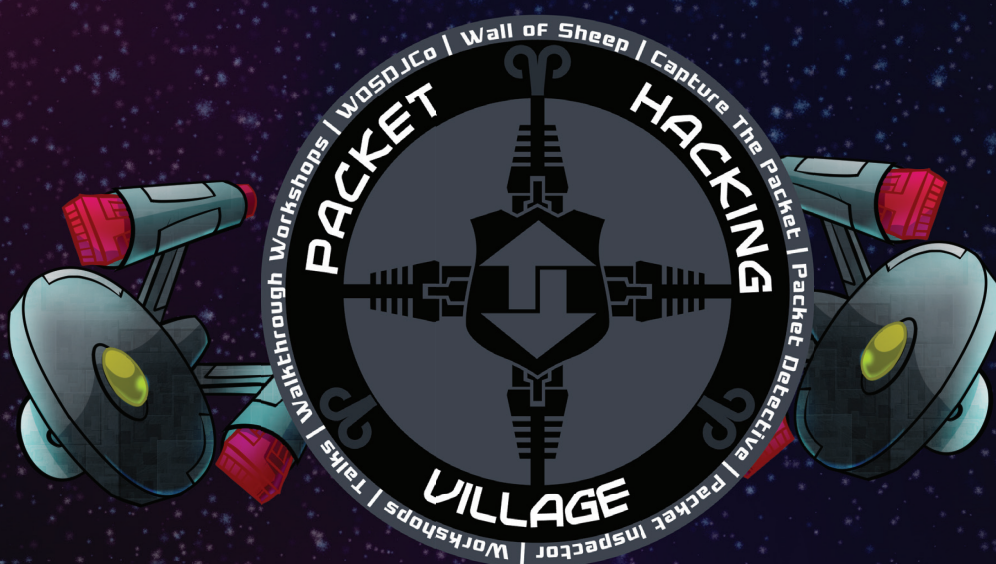
Twitter: [@r00tzasylum](https://twitter.com/r00tzasylum)

## RECON VILLAGE

Friday: 12:00 - 18:00, Saturday: 10:00 - 18:00, Sunday: 10:00 - 13:00

Location: Planet Hollywood, Celebrity 5 and Some Celebrity 6

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, Beginner Sessions, CTFs with a common focus on Reconnaissance. The village is meant for professionals interested in areas of Open Source Intelligence (OSINT), Threat Intelligence, Reconnaissance, and Cyber Situational Awareness, etc. with a common goal of encouraging and spreading awareness around these subjects.



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 26th floor in Bally's.

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. 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.

# CAPTURE THE PACKET

## Capture The Packet - CTP

Come compete in the world's most challenging cyber defense competition based on the Aries Security Cyber Range. Tear through the challenges, traverse a hostile enterprise class network, and diligently analyze what is found in order to make it out unscathed. Not only glory, but prizes await those that emerge victorious from this upgraded labyrinth, so only the best prepared and battle hardened will escape the crucible. Follow us on Twitter or Facebook (links below) to get notifications for dates and times your team will compete, as well as what prizes will be awarded.

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 - WoSDiCo

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.



/wallofsheep



@wallofsheep





# PACKET INSPECTOR

ARIES SECURITY

## Packet Inspector - Beginner/Intermediate

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

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

# PACKET DETECTIVE

ARIES SECURITY

## Packet Detective - Intermediate/Advanced

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.

# WALKTHROUGH WORKSHOPS

## Walkthrough Workshops - Learn to build Honey Pot's

The Packet Hacking Village brings you the 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

### PHV Talks

We have world class speakers presenting 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/dc27>*



## PHV WORKSHOPS

### PHV Workshop

A returning favorite from previous years, we have hands-on labs and training sessions from an amazing line-up of instructors covering beginner to advanced level material.

*Updated schedule available at: <https://wallofsheep.com/pages/dc27>*



/wallofsheep



@wallofsheep



# VILLAGES

Village Schedule: <https://reconvillage.org/talks.html>

Website: <https://reconvillage.org>

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

## RED TEAM OFFENSE VILLAGE

Friday: 09:00 - 19:00, Saturday: 09:00 - 19:00, Sunday: 09:00 - 13:00

Location: Flamingo, Laughlin I and II

The Red Team Offense Village is a first year village at DEF CON. The Village goal is to give back to the community by helping others learn how to build or improve their RED TEAM concepts, skills, and tool kits.

Things happening in the village will include:

### RED TEAM STATIONS

The village will have 5 different stations with numerous exercises where participant can practice their skills and learn new ones. Exercises include red team methodologies, several exploitation, evasion, persistence and obfuscation techniques, and much more.

### TECHNICAL PRESENTATIONS AND DISCUSSIONS

The village has a dedicated area for numerous talks from Red Team experts all three days.

Website: [www.RedTeamVillage.io](http://www.RedTeamVillage.io)

## ROGUE'S VILLAGE

Friday: 13:00-19:00, Saturday: 13:00-19:00, Sunday:-

Location: Flamingo, Carson City II

Rogues Village is a place to explore alternative approaches to existing security concepts by looking to non-traditional areas of knowledge. Incorporating expertise from the worlds of magic, sleight of hand, con games and advantage play, this village has a special emphasis on Social Engineering and Physical Security. Talks will cover topics ranging from secret communication methods used by nineteenth century mediums to physical techniques of a modern pickpocket. Demos and workshops will also give attendees hands-on opportunities to experience these non-traditional methods.

Village Schedule: [www.foursuitsmagic.com/roguesvillage](http://www.foursuitsmagic.com/roguesvillage)

Website: [www.foursuitsmagic.com/roguesvillage](http://www.foursuitsmagic.com/roguesvillage)

Twitter: [www.twitter.com/roguesvillage](https://twitter.com/roguesvillage)

## SOCIAL ENGINEERING VILLAGE

Thursday: 10:00 - 19:20, Friday: 10:00 - 19:20, Saturday: 10:00 - 19:20, Sunday: 10:00 - 13:00

Location: Bally's, Jubilee Tower - Las Vegas BR - 3rd Floor

Established at DEF CON 18 the SEVillage at DEF CON has been the one-stop shop for all things social engineering. From our humble beginnings with a small room and our sound proof booth to now running 4 events and a "Human Track" where social engineering talks are given. The SEVillage at DEF CON 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!

Village Schedule: <https://www.social-engineer.org/sevillage-def-con/>

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

## SKYTALKS 303

Thursday: 18:30 - end of a party?, Friday: 09:00 - 19:00, Saturday: 09:00 - 19:00, Sunday: 09:00 - 14:00

Location: Bally's, Jubilee Tower - Pacific BR - 2nd Floor

Skytalks is an ongoing talk series presenting sensitive and fringe talks on a number of topics. In our 12th year at DEF CON, we are proud to bring you the best of Old School DEF CON. No shills. No Bullshit. No cameras. No Kidding.

Website: Twitter: @dcskytalks

Twitter: <https://skytalks.info>

## SOLDERING SKILLS VILLAGE

Friday: 10:00 - 19:00, Saturday: 10:00 - 19:00, Sunday: 10:00 - 13:00

Location: Bally's, Event Center

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. We have a variety of parts and random hardware to include in or support hacking projects.

## TAMPER-EVIDENT VILLAGE

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

Location: Bally's, Platinum BR

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

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

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

- \* Tamper-Evident Contest; a full-featured tamper challenge. New for this year: KING OF THE HILL! 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.

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

\* For your viewing pleasure, collections of high-security tamper-evident seals from around the world.

\* 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.

## VOTING MACHINE HACKING VILLAGE

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

Location: Planet Hollywood, Wilshire Ballroom A-B

The Voting Machine Hacking Village ("Voting Village") returns for its third year at DEF CON! As the only public third-party assessment of voting infrastructure in the world, the Voting Village attracts thousands of white hat hackers, government leaders, and members of the media to partake in the mission of rigorously researching voting systems and raising awareness of voting vulnerabilities.

The Voting Village gives hackers a unique opportunity to directly audit voting machines and other election equipment. With the 2020 elections looming and efforts to combat election vulnerabilities ongoing at the state and federal levels, the educational mission of the Voting Village remains as critical as ever.

## VOTING VILLAGE SPEAKER ROOM

Friday: 10:00 - 18:00

Location: Planet Hollywood, Melrose 4

As in previous years, the Voting Village will include a day-long set of panels and keynotes where attendees can hear from cyber and national security experts, elected officials, and hackers. Among this year's selection of speakers are state and local election officials, homeland security leaders, world-renowned hackers, media personalities – and much more.

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

## VARIETY EXPLOITATION VILLAGE

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

Location: Bally's, Event Center

Powered by VXRL Hong Kong – VXRL is founded by a group of passionate cybersecurity researchers and white-hat hackers in Hong Kong. The team has deep expertise in software and hardware security, and hands-on domain knowledge in several vertical industries. VXRL mission is to make the cyberspace a safe place for the future. The VX(Variety eXploitation) Village will be powering an in-depth hands-on playground.

Village Schedule: [www.dcvxv.org](http://www.dcvxv.org)

Website: [www.dcvxv.org](http://www.dcvxv.org)

## WIRELESS VILLAGE

Thursday: 12:00-17:00, Friday: 10:00 - 19:00, Saturday: 10:00 - 19:00,

Sunday: 10:00 - 13:00

Location: Ballys, Palace Meeting Rooms 1-7

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)? RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Wireless Capture the Flag (WCTF) at DEF CON in the Wireless Village. We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The WCTF can be completely done with a little knowledge, a pentester's determination, and \$50 or \$5000 worth of equipment. The key is to read the clues and determine the goal of each challenge. Each WCTF event begins with a presentation: How to WCTF.

There will be clues everywhere, and we will provide periodic updates. Make sure you pay attention to what's happening at the WCTF desk, on Twitter: @wctf\_us, @rfhackers, and the interwebz, etc. If you have a question ASK! We may or may not answer at our discretion. FOR THE NEW FOLKS Bring your laptop, wifi dongles, SDR, Bluetooth, IR, and anything else you think may help. Read the presentations at: <http://wctf.us/resources.html> Check out the resources at: <http://sdr.ninja/training-events/sdr-wctf/> Read the Blog at: <https://wirelessctf.blogspot.com/> Follow on Twitter: @wctf\_us, @WIFI\_Village, and @rfhackers

Village Schedule: <https://www.wirelessvillage.ninja/speakersched.html>

Website: @wifi\_village

Twitter: @wctf\_us

Other: @rfhackers



## NEW ERA, SAME OVERFLOW: DEF CON CTF 27

Last year at DC 26, the Order of the Overflow hosted their first DEF CON CTF finals. During the 24 hours of game competition from Friday to Sunday, the teams battled it out through exploiting a JavaScript interpreter, reversing Objective-C, writing polyglot shellcode in esoteric architectures (e.g., PDP-1, IBM 1401, and MIX), and many other heroic feats of pwning. DEFKOROOT emerged victorious, dominating the competition by capturing 2,421 flags.

Throughout the contest, the Order brutally held onto control through an iron fist and unassailable API endpoints. But now, the Order has seen the light—the glittering lights of humanity's bright future. Only by cooperation and working together can we achieve the next phase of humanity's evolution: vulnerability-free software. If we can set aside our petty differences that only serve to divide and weaken us, we can achieve this glimmering future.

Imagine hackers of all stripes: Emacs/Vim, Linux/Windows, Android/iOS, Intel/ARM, Nvidia/AMD, NetWare/NT, Firefox/Chrome, Azure/AWS, radare2/IDA Pro, all extinguishing their flame wars in the noble pursuit of hacking a better future. That time can be now, you can be those hackers.

Join us in harmony as we revel in the glory of a secure future. All are equal, and all are welcome. Let's go where no one has gone before:

Hack long, and prosper.



## 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. We have introduced twists 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) or by winning HITCON CTF, RuCTfE, C3CTF, PlaidCTF, OCF, or, BCTF.

This year, more than 1,200 teams tried to qualify, and 156 solved more than 3 challenges. Among these worthy competitors we have gathered the world's top 16 teams:

A\*0\*E

CGC

HITCON BFKinesis

hxp

KalsHack GoN

mhackeroni

Plaid Parliament of Pwning

r00timentary

r3kapig

saarsec

Samurai

Savercloud

SeoulPlusBadAss

Shellphish

Tet Deliverers

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, 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>

We hope to see you play in finals next year!

# DC27 CTF



# CONTESTS & EVENTS

## AI VILLAGE CTF

Location: AI Village

Do you want to test your mettle at security machine learning? Want to try your hand at detecting spam and malware? Or do you want to attack the spam filter or next gen AV? Or even attack the AI itself. The AI Village CTF is here for all your red & blue AI needs. There is a challenge for everyone and a learning curve for beginners. We also have cutting edge problem for experts to try their hands at.

More Info: <http://aivillage.org>

DEF CON Forums: <https://forum.defcon.org/node/227728>

DEF CON Forums: <https://forum.defcon.org/node/226665>

Twitter: @CarHackVillage

## BEVERAGE COOLING CONTRAPTION CONTEST

Location: Contest Stage (PH Mezzanine)

Friday: 1300-1500

Trump is trumping, Theresa May is waffling, Vladimir Putin is meddling, Xi Jinping reeducating, Angela Merkel is resigning, but worst of all the beverage isn't cooling! I've tried everything! I built a wall around it! I posted misleading information on social media about it! I locked it in a closet and sang inspiring nationalistic songs at it for five hours! I tried to convince it to just be cold but gave up! Nothing is working!

The BCCC returns to DEF CON bringing warm beverage somebody needs to make cold. That somebody could be you! Didn't bring a contraption? No problem! You can enter the hacked category and only compete against others who build their contraption at the convention. The BCCC is a light hearted contest with a crazy yet easy going atmosphere. We are always looking for new faces and hope to see you there!

More Info: <https://bccweb.wordpress.com/>

DEF CON Forums: <https://forum.defcon.org/node/227730>

## CMD+CTRL CYBERRANGE

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

CMD+CTRL is unleashing two new vulnerable apps at DEF CON 27, these aren't your grandfather's CTFs. We've created an Android app and a tough client side JS app & API ready to be hacked.

As always, CMD+CTRL challenges are automatically detected and scored, awarding points with every successful exploit. There are over 100 different challenges, including authentication vulns, cipher cracking, OWASP Top 10 weaknesses, and more. There are basic challenges and getting started guides for beginners, as well fortified defenses that will challenge even the most clever hackers.

Come apply your Red Team kung fu on the latest AppSec Cyber Range!

Twitter: @SecInnovation

## COINDROIDS

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

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 through manual labor or the sweet power of automation.

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.

More Info: <https://www.coindroids.com>

DEF CON Forums: <https://forum.defcon.org/node/227724>

Twitter: @coindroids

## CAR HACKING VILLAGE CTF

Location: Car Hacking Village

Come learn, hack, play at the Car Hacking Village. The village is an open, collaborative space to hack actual vehicles that you don't have to worry about breaking! Don't have tools? We'll loan you some. Never connected to a car? We'll show you how. Don't know where the controllers are? We'll show you how to take it apart.

Additionally we'll host a Donkey Car race. Check out our web site for up to date info.

Want to race? Check out of full car simulator(s).

Want to learn more about automotive hacking and cyber security? Check out our talks.

Want to hack mobility scooters? Yes! We'll do that to.

Also, check out the CHV CTF.

More Info: <http://www.carhackingvillage.com>

## CRACK ME IF YOU CAN

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

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.

# CONTESTS & EVENTS

But now, you have to crack all these hashes.

In it's 8th 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 2019, 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 3080 Tis 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 FortNight, there are passwords to crack!

More Info: <https://contest.korelogic.com/>

DEF CON Forums: <https://forum.defcon.org/node/227733>

Twitter: @crackmeifyoucan

## CREATIVE WRITING SHORT STORY CONTEST

Location: Online

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.

This year's winners:

1st Place: "Dye Sublimation" by Selene Sun

2nd Place: "Parsnips" by David Hash Miller

People's Choice: "Red Balloons over China" by FengJiu

More Info: May 1, 2019 - June 15, 2019

DEF CON Forums: <https://forum.defcon.org/node/227709>

Twitter: @dcshortstory

## DARKNET PROJECT

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

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.

More Info: <https://dcdark.net>

DEF CON Forums: <https://forum.defcon.org/node/227711>

Twitter: @DCDarknet

## DEF CON BEARD CONTEST

Location: Contest Stage (PH Mezzanine)

Saturday: 1300-1500

The annual celebration of facial hair at DEF CON. There are four categories for entry

Full Beard - meant for the truly hairy and bearded.

Partial Beard - For those sporting Van Dykes, Goatees, Mutton Chops, and more.

Mustache Only - Bring us your handlebars, Fu Manchus, or whatever else adorns your upper lip.

Freestyle - Anything goes, the wilder the better.

So fertilize your face and join us. Sign-up early via <https://goo.gl/forms/cSb3p5A7A0HwD3wG2> or sign-up on site. No more than 2 categories per contestant please.

More Info: <http://www.dcbear.com>

DEF CON Forums: <https://forum.defcon.org/node/227712>

## DEF CON HAM RADIO FOX HUNTING CONTEST

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

In the world of amateur/ham 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 transmit on a different frequency, requiring them to "hunt" for transmissions.

Each transmitter when located will have a small message encoded next to the transmitter, which will decode to a unique web address which will contain a flag. Finding the flag will verify they have found the transmitter.

Each day the transmitters will be moved to new locations and a new flag will need to be found.

Scores will be kept for each day, with a daily



winner, and an all-round winner. Participants will receive a ham radio themed participation ribbon, and daily winners and all-round winners (1st - 3rd place) will get this year's engraved silly trophy. 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.

More Info: <http://defcon26foxhunt.com/>

DEF CON Forums: <https://forum.defcon.org/node/227734>

## DEF CON SCAVENGER HUNT

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

It is the distant dystopian future, the year 2019; Las Vegas, Nevada. You have been tasked with collecting as much as possible from our list; including a Nexus 6, a synthetic owl, and a Sean Young blow-up doll. Let nothing stand in your way. Be it replicant, retire them; be it goon, beer them. Your time is limited, go now, you have only from 10AM Friday until noon on Sunday. Find us in the contest area to administer your submissions; be advised trigger warnings are in full effect.

More Info: <http://defconscavhunt.com>

DEF CON Forums: <https://forum.defcon.org/node/227658>

Twitter: @defconscavhunt

## DRUNK HACKER HISTORY

Location: Contest Stage (PH Mezzanine)

Saturday: 2200-2400

One night only at DEF CON 27, Drunk Hacker History is back by popular demand for a 5th triumphant year! The past four years proved to the entire planet 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 is filled with mephitic adventures, quarter-truths, poor life choices, incontinence, and various forms of C2H6O. This year, we will journey to the land of the shadows 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 candy from Japan, deli meat sliced by a sword, Orange Whips, and feats of strength, you won't want to miss the return of Drunk Hacker History! Presented in DEF CON 4D, 5G, GPRS and made possible by a grant from <https://ghost.express>. Note: If you arrive early, you might enjoy the festive dancing, music and handfuls of Cinnamon Life cereal. Yum!

DEF CON Forums: <https://forum.defcon.org/node/227713>

Twitter: @DrunkHackerHist

## DUNGEONS@DEF CON

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 10:00-20:00, Sunday: 1000-1200

Dungeons@DEF CON is an RPG style puzzling campaign for 1-4 players. - .... / ... / - . . . . . / - - / ... / ... - . . . .

More Info: [dungeonsatdefcon.com](http://dungeonsatdefcon.com)

DEF CON Forums: <https://forum.defcon.org/node/227714>

## EFF TECH TRIVIA

Location: Contest Stage (PH Mezzanine)

Friday: 1700-1900

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. \* For this year we have updated the trivia to reflect the latest in security and make it even better!

More Info: <https://eff.org>

DEF CON Forums: <https://forum.defcon.org/node/227725>

Twitter: @eff

## HACK THE PLANET

Location: ICS Village

Hack the Plan[e]t Capture the Flag (CTF) contest will feature Howdy Neighbor and the Industrial Control System (ICS) Range. This first of its kind CTF will integrate both Internet of Things (IoT) and ICS environments with interactive components for competitors to test their skills and knowledge.

Howdy Neighbor is an interactive IoT CTF challenge where competitors can test their hacking skills and learn about common oversights made in development, configuration, and setup of IoT devices. Howdy Neighbor is a miniature home - made to be "smart" from basement to garage. It's a test-bed for reverse engineering and hacking distinct consumer-focused smart devices, and to understand how the (in)security of individual devices can implicate the safety of your home or office, and ultimately your family or business. Within Howdy Neighbor there are over 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 competitors ability to find vulnerabilities in an IoT environment. Howdy Neighbor's challenges are composed of a real or simulated devices controlled by an App or Network interface and additional hardware sensors; each Howdy Neighbor device contains 1 to 3 staged vulnerabilities which when solved present a key for scoring/reporting that it was discovered.

# CONTESTS & EVENTS

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.

More Info: <https://www.icsvillage.com>

DEF CON Forums: <https://forum.defcon.org/node/227732>

Twitter: @ics\_village

## HACKER JEOPARDY

Location: Contest Stage (PH Mezzanine)

Friday: 2000-2200, Saturday: 20:00-22:00

DEF CON's longest running show Hacker Jeopardy turns 25 this year, and it's going to be HUUUGE! For our Silver Anniversary, we conducted qualifying rounds around the world and invited the winners. Three teams of three will compete in this hilarious parody game, with additional points awarded for beer consumed. Anything can happen on stage (we even had a marriage proposal!) – you just gotta be there (our sponsors give away AWESOME swag.) Adult-themed, this show is not for minors and emotionally sensitive persons. We're offended if you're not offended. Be there. Aloha

More Info: [www.hackerjeopardy.com](http://www.hackerjeopardy.com)

DEF CON Forums: <https://forum.defcon.org/node/227657>

Twitter: @hackerjeopardy

## HACKFORTRESS

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

Hackfortress is a unique blend of Team Fortress 2 and a computer security contest. Teams are made up of 6 TF2 players and 4 hackers, TF2 players duke it out while hackers are busy solving puzzles. As teams start scoring they can redeem points in the hack fortress store for bonuses. Bonuses range from crits for the TF2, lighting the opposing team on fire, or preventing the other teams hackers from accessing the store.

More Info: <http://hackfortress.net>

DEF CON Forums: <https://forum.defcon.org/node/227715>

## H@CK3R RUNW@Y

Location: Contest Stage (PH Mezzanine)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

In the times I've been to DEF CON, I've seen a lot of cool styles around the conference and at the parties. People with brooches that counted handshakes, skirts with interactive LEDs, etc. This contest is to celebrate all of the cyber fashionistas out there. Whether it's something that lights up, interactive, multipurpose, or just geeky but aesthetically pleasing. Items entered can be in the form of clothing, shoes,

jewelry or accessories. Participants can predesign their entry or create something on site during DEF CON as long as it's before final votes.

There are four (4) categories for predesign and one (1) for anything designed during contest hours:

- § Digital (electronic, led, etc)
- § Smart wear (interactive, temperature sensing, mood changing, etc)
- § Aesthetics (3d printed, geeky wear, passive design)
- § Physical security (lock picks, shims, card skimmers)
- § Live creations

Entries will be judged based on the following criteria:

- § Uniqueness
- § Trendy
- § Practical
- § Couture
- § Creativity
- § Relevance
- § Originality
- § Presentation
- § Mastery

Twitter: @Hack3rRunway

Homebrew Hardware Contest

Location: Contest Stage (PH Mezzanine)

Saturday: 1500-1700

Are you fulfilling the promise of tomorrow's technology today? Are you etching circuit-boards in your lab, or soldering in a toaster oven in your garage? Are you hosting a MUD on your helmet, or making malicious USB hardware? Did you make something to help you in your every day life, a unique wearable, or something really nefarious?

We want to see the awesome things you've been building over the last year. The HomebrewHardware competition is a place to showcase your skill, techniques, and project.

Rules:

1. Bring your hardware, and proof of how you made it (video, pictures, etc.)
2. Each entry will be given 5 minutes to discuss what they built, how they built it, and show a practical demonstration.
3. A panel of judges will rank entries based on a number of categories including: innovativeness, construction techniques, utility, and aesthetics.
4. Prizes will be awarded for 1st, 2nd, and 3rd place.
5. Entries can submit early (watch our twitter) but must be present to talk through their hardware on stage.
6. Entries can be teams or individuals.
7. Entries can leverage commercial parts and gear, but should strive to meet the spirit of homebrew!
8. No badges, please. We <3 badgelife, but there are already some awesome contests for them.

DEF CON Forums: <https://forum.defcon.org/node/228300>



Twitter: @homebrewharwa1

## HOSPITAL UNDER SIEGE

Location: BioHacking Village

Adversaries have gained a foothold in your local hospital and are increasing their control over clinical systems and medical devices. Soon they make it clear they're not after patient records or financial information, but are out to disrupt care delivery and put patients lives at risk. Your team received an urgent request to use your blue, red, and purple team skills to defend against the escalating attacks, attempt to unmask the adversary, and - above all - protect patient lives.

Hospital Under Siege is a scenario-driven Capture the Flag contest run by the Biohacking Village, pitting teams of participants against adversaries and against a clock, to protect human life and public safety. Participants will compete against each other on both real and simulated medical devices, in the fully immersive Biohacking Village: Device Lab, laid out as a working hospital. Teams of any size are welcome, as are players from all backgrounds and skill levels. Challenges will be tailored for all skill levels and draw from expertise areas including forensics, RF hacking, network exploitation techniques, web security, protocol reverse engineering, hardware hacking, and others. You will hack actual medical devices and play with exotic protocols like DICOM, HL7 and FHIR.

More Info: <https://www.vilageb.io>

DEF CON Forums: <https://forum.defcon.org/node/228301>

Twitter: @dc\_bhv

## MAPS OF THE DIGITAL LANDS

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

This is a contest where contestants will draw a diagram of the provided network scenarios within the time allotted and judges will determine the winners based on feasibility, practicality, readability, whether or not the key components have been included and clearly identified, and most importantly the least amount of room for hackers to take over their proposed network. Prizes will be awarded for the best of each scenario which will all have increasing difficulties.

DEF CON Forums: <https://forum.defcon.org/node/228302>

## OPENTCF

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

OpenCTF, a hacking contest built on the principle of inclusion with challenges for all skill levels, is returning to DEF CON this year under new management. OpenCTF will continue to be open to all, so if you're new to CTF come talk to us and we'll

help you get started or find a team, but bring your dedication if you aspire to win. Neg9, long time players and former winners, will be organizing and hosting the contest. Get ready for the next level!

DEF CON Forums: <https://forum.defcon.org/node/227729>

## OPENSOC BLUE TEAM CTF

Location: Blue Team Village

OpenSOC is a Digital Forensics, Incident Response (DFIR), and Threat Hunting challenge meant to teach and test practical incident response skills in an environment that closely resembles a real enterprise network. This virtual environment is a scaled down version of what you would find in an enterprise network, including: workstations, servers, firewalls, email, web browsing, user activity, etc. Simulated users are browsing the Internet, downloading files, watching videos, and accessing LAN resources. This creates a high fidelity training environment for unleashing real-world attacks and testing a responder's ability to filter out the noise and find malicious activity on the network.

This isn't just another CTF. We've built this platform to train real-world responders to handle real-world situations.

What's even better? 100% of the security tools demonstrated on OpenSOC are FREE and OPEN SOURCE! These projects include Wazuh + ossec, Kolide + osquery, Suricata, Snort, Moloch, OPNsense, pfSense and Graylog bringing it all together in an awesome way.

The Challenge:

- Given an initial IOC's (indicator of compromise (or pivot point)), identify attacks that are being carried out against and within the enterprise environment.
- Trace the attackers throughout the kill chain, submitting key IOCs and observables to the scoreboard as you reveal their tactics.
- Reverse engineer any artifacts connected to hostile activities.
- Perform forensics analysis on PCAPs (Packet Captures), memory images, etc.

Win awesome prizes, learn new skills, and get experience with some of the best OPEN SOURCE tools for SecOps!

More Info: <https://opensoc.io>

DEF CON Forums: <https://forum.defcon.org/node/228303>

Twitter: @recon\_infosec

## OSINT CTF FOR MISSING PERSONS

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

Want to help solve actual crimes? Want to be the hero that brings home a loved one?

Join us for the 2nd year of the OSINT

# CONTESTS & EVENTS

## CTF for Missing Persons Challenge!

Each day we will present 8 real missing persons for you to track and submit open source intelligence into our CTF platform.

Prizes awarded at the end of each day include a virtual training voucher from the highly respected Michael Bazzell of Intel techniques as well as licenses for Hunchly, the software every OSINT operator needs.

This is fantastic opportunity to get into the OSINT community, learn intelligence gathering and to become a hero.

Get your team together and join us at the Trace Labs table in the contest area to get started.

If you want to get familiar with Trace Labs, our community and the CTF, sign up here and we will answer any of your questions on our Slack channel: <https://www.tracelabs.org/accounts/register/updated-description>

More Info: [www.tracelabs.org](http://www.tracelabs.org)

DEF CON Forums: <https://forum.defcon.org/node/228304>

Twitter: @tracelabs

## RED ALERT ICS CTF

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

Red Alert ICS CTF is based on ICS test bed (simulation) so all participant can hack actual devices in ICS/SCADA environment. We create virtual SCADA environment in order for participants to penetrate several layers of security to gain points, and eventually gain control of SCADA system. Some challenges include Bypassing Airgap, ICS protocols and PLC & HMI softwares, Forensics, and Cyber Incidents (including classic and basic challenge, reversing and web).

More Info: <http://icssecurity.net/ctf>

DEF CON Forums: <https://forum.defcon.org/node/227727>

## SCHEMAVERSE

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

The Schemaverse [skee-muh vurs] is a space battleground that lives inside a PostgreSQL database. Mine the hell out of resources and build up your fleet of ships, all while trying to protect your home planet. Once you're ready, head out and conquer the map from other DEF CON rivals. New this year, time travel!

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!

More Info: <https://schemaverse.com>

DEF CON Forums: <https://forum.defcon.org/node/227718>

Twitter: @schemaverse

## SECTF

Location: SE Village

The SECTF is social engineering's premier contest in which selected participants are tasked and judged on legally obtaining information, known as flags, about specified corporate targets in two parts. First, participants prepare and submit reports detailing flags they discovered through open-source intelligence (OSINT) gathering in the weeks leading up to the competition. Second, on the SEVillage's main stage, participants are provided 20 minutes to call the target companies in real-time from a live-streamed sound-proof call box, and attempt to obtain those same flags they found via OSINT. The SEVillage at DEF CON 27 will host its 9th annual SECTF.

## SECTF4KIDS

Location: SE Village

In the SECTF4Kids, participants aged 5-12 are given a variety of tasks that involve critical thinking, team work, and problem-solving skills (e.g., lock picking, cipher cracking, elicitation). To win the SECTF4Kids, they must race against the clock, and other teams, to complete all the tasks.

## SECTF4TEENS

Location: SE Village

In the SECTF4Teens, participants aged 13-17 are given a variety of tasks that involve research, critical thinking, and problem-solving skills (e.g., OSINT, lock picking, cipher cracking, elicitation).

An increased challenge from the SECTF4Kids, many of our previous kid-competitors have now graduated to this more competitive, independent contest.

## SECURE CODE REVIEW CHALLENGE

Location: AppSec Village

Secure Code Review is an important "tool" in an AppSec practitioners tool box. This contest aims to challenge contestants on performing Secure Code Review and crown someone supreme Secure Code Reviewer. Contestants will be asked questions after being presented with merge requests taken from Open Source projects where a confirmed vulnerability has been addressed or CVE descriptions.

More Info: <http://www.appsecvillage.org/threatmodeling/>

DEF CON Forums: <https://forum.defcon.org/node/228305>

Twitter: @AppSecVillage



## SOHOPELESSLY BROKEN

Location: IoT Village

A DEF CON 24-26 Black Badge Village CTF, players compete against one another by exploiting off-the-shelf IoT devices. These 25+ devices all have known vulnerabilities, but to successfully exploit these devices requires lateral thinking, knowledge of networking, and competency in exploit development. CTFs are a great experience to learn more about security and test your skills, so join up in a team (or even by yourself) and compete for fun and prizes! Exploit as many devices as you can across three network segments. 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>. The winners who score the highest on their judged entries will be rewarded with prizes. Contestants will need to provide proof that they disclosed the vulnerability to the vendor.

More Info: <http://www.sohopelesslybroken.com>

DEF CON Forums: <https://forum.defcon.org/node/227731>

Twitter: @sohobroken

## SPELLCHECK: THE HACKER SPELLING BEE

Location: Contest Stage (PH Mezzanine)

Friday: 1500-1700

A year ago, under dystopian conditions, one worthy speller lifted the champion's belt above her head. The ascent of that gleaming trophy parted the clouds of confusion and brought with it the promise of a new day. Through the bee, the Cybersecurity Style Guide strengthened the emerging union between humans and technology. Now, that hope-filled guide has spawned an itty-bitty helper — a fierce little dictionary to augment your word processor's native spell check list.

In celebration of a blossoming age of digital-analog cooperation, we're taking time this golden summer to revisit the high drama and awkward humor of the good old-fashioned spelling bee.

We'll use the most recent version of the Cybersecurity Style Guide for the official spelling of each term. Rounds will increase in difficulty and eventually include saying proper capitalization out loud for tricky everyday terms and rare attack vectors alike.

25 challengers can compete! Sign up in advance by emailing [style@bishopfox.com](mailto:style@bishopfox.com) before August 7, or just come to the event a little early and volunteer on the spot. All spellers will get participation badges, and the winner will receive a unique prize.

It's a lovely day. Take a stroll with us down random-access memory lane.

More Info: <http://cybersecuritystyleguide.com>

DEF CON Forums: <https://forum.defcon.org/node/227735>

## SPY CONTEST (WHO'S THE BEST SOCIAL ENGINEER)

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

This contest is trying to figure out which individual or team is the best social engineer in the DEF CON kingdom. You will receive a URL used to generate points for your score. Using any means necessary via social engineering (aka Phishing, Phone Calls, Physical Face-to-Face Requests, etc.), your goal is to generate the highest number of unique visits to your URL from DEF CON attendees. There will be extra points awarded for specifically named "Monsters" such as DEF CON staff, specific high profile individuals, etc.

DEF CON Forums: <https://forum.defcon.org/node/228306>

## TTELECHALLENGE

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

Would you like to play a game? The TeleChallenge is a fully immersive puzzle challenge. Playable via your phone, the Challenge combines real-world clues with phreakable systems in an epic battle of wits and skill. While anyone with a phone can play, this is not a simple Challenge. Winning will require an intense level of dedication from you and your team. See you on the game grid!

More Info: <https://telechallenge.org>

DEF CON Forums: <https://forum.defcon.org/node/227720>

Twitter: @telechallenge

## THE D(STRUCTION)20 CTF

Location: Contest Stage (PH Mezzanine)

Saturday: 1100-1300

Are you tired of CTFs where contestants' computers aren't in danger of being smashed with a sledgehammer by a person wearing a hot dog costume? Do normal CTFs that don't decide the fate of their competitors at random with a novelty oversized 20-sided die bore you? Then come see the only CTF where the stack isn't the only thing being smashed:

### The d(struction)20 CTF!

Part CTF, part lemon race, part game show, part demolition derby, the D(struction)20 CTF is a contest to build an affordable, low-cost, usable, and powerful hacking platform, and compete with it! Periodically during the competition, a random contestant from the leaderboard will be chosen to 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

# CONTESTS & EVENTS

damage will be inflicted! Otherwise, the d20 of Destruction will decide what type of damage will be done to their rig. 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!

DEF CON Forums: <https://forum.defcon.org/node/227710>

Twitter: @d20ctf

## THE GOLD BUG - CRYPTO & PRIVACY VILLAGE PUZZLE

Location: Crypto Village  
TBD

More Info: <http://goldbug.cryptovillage.org>

DEF CON Forums: <https://forum.defcon.org/node/227723>

Threat Modeling Challenge

Location: AppSec Village

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist. As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner.

More Info: <http://www.appsecvillage.org/threatmodeling/>

Twitter: @AppSecVillage

## TINFOIL HAT

Location: Contest Floor (PH Celebrity Ballroom)  
Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

NSA Mind control rays have you down? Those pesky grays trying to control your neural cortex? Fear not, for we here at the Tinfoil Hat contest have your back. Come find us in the contest area, and we'll have you build a Tinfoil hat which is guaranteed to provide top quality protection for your noggin. How you ask? SCIENCE!

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

DEF CON Forums: <https://forum.defcon.org/node/227736>

Twitter: @dc\_tin\_foil\_hat

## WARLOCK GAM3Z CTF

Location: Contest Floor (PH Celebrity Ballroom)

Friday: 1000-2100, Saturday: 1000-2100, Sunday: 1000-1200

warl0ck gam3z CTF is a hands-on 24/7 throw-down, 3 time black badge 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. There is always on onsite/online moderator to assist participants that may be experiencing issues as well. All events highlights that occur on the game board are sent o to Twitter as they happen. Additionally, our Facebook site will be populated with information regarding the challenge and the current state of events.

More Info: <https://www.facebook.com/Gam3zInc>

DEF CON Forums: <https://forum.defcon.org/node/227721>

Twitter: @gam3z\_inc

## WHOSE SLIDE IS IT ANYWAY?

Location: Contest Stage (PH Mezzanine)  
Friday: 2200-2400

**The What:** "Whose Slide Is It Anyway?" is an unholy union of improv comedy, hacking and slide deck sado-masochism.

**The How:**

Our team of slide monkeys will create a stupid amount of short slide decks on whatever nonsense tickles our fancies. Slides are not exclusive to technology, they can and will be about anything. Contestants will take the stage and choose a random number corresponding to a specific slide deck. They will then improvise a minimum 5 minute / maximum 10 minute lightning talk, becoming instant subject matter experts on whatever topic/stream of consciousness appears on the screen.

**The Why:**

Whether you delight in the chaos of watching your fellow hackers squirm or would like to sacrifice yourself to the Contest Gods, it's a night of schadenfreude for the whole family. Sign ups will be the day of the contest with some special ways to secure your spot early.



### New This Year:

Battle of Champions! Anyone who has won a version of Whose Slide at other conferences during the last year will compete against our previous Vegas champs in a Slide Slaughter Royale.

Guerrilla Talks. Have portable projector and sound, will travel. :)

More Info: <http://www.improvhacker.com>

DEF CON Forums: <https://forum.defcon.org/node/227722>

## WIRELESS CAPTURE THE FLAG

Location: Wireless Village

Do you have what it takes to hack WiFi, Bluetooth, and Software Defined Radio (SDR)?

RF Hackers Sanctuary (the group formerly known as Wireless Village) is once again holding the Wireless Capture the Flag (WCTF) at DEF CON in the Wireless Village.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The WCTF can be completely done with a little knowledge, a pentester's determination, and \$50 or \$5000 worth of equipment. The key is to read the clues and determine the goal of each challenge. Each WCTF event begins with a presentation: How to WCTF. There will be clues everywhere, and we will provide periodic updates. Make sure you pay attention to what's happening at the WCTF desk, on Twitter: @wctf\_us, @rfhackers, and the interwebz, etc. If you have a question ASK! We may or may not answer at our discretion.

### FOR THE NEW FOLKS

Bring your laptop, wifi dongles, SDR, Bluetooth, IR, and anything else you think may help.

Read the presentations at: <http://wctf.us/resources.html>

Check out the resources at: <http://sdr.ninja/training-events/sdr-wctf/>

Read the Blog at: <https://wirelesscf.blogspot.com/>

Follow on Twitter: @wctf\_us, @WIFI\_Village, and @rfhackers

More Info: <https://wctf.us/>

DEF CON Forums: <https://forum.defcon.org/node/228630>

Twitter: @wctf\_us

teams can use as many actors and extras as they want.

Open to all.... (zero experience, students, amateurs, professionals).

Team registration starts Thursday morning. Get the rules, get your official "I'm making a movie so watch out" orange t-shirt\*, deal with the monkey wrenches, and go out and get it all done by Saturday afternoon.

Entries premiered Saturday evening, August 11, in Planet Hollywood, Melrose 4.

Entries screened prior to commencement of DEF CON 27 closing ceremony on Sunday, August 12.

Prizes include 5 Human Badges for DEF CON 28, 1 year Subscription Adobe Premier, VideoMaker Magazine subscriptions (and other cool TBD stuff).

Extras and actors needed.

You don't have to join a team to have some filmmaking fun at DEF CON. You could be an extra, or even an actor, in one of the films being made here at DEF CON. Sign up Thursday morning or ask one of the conspicuously clad orange t-shirt wielding teams you may see during the Con.

### \*ATTENTION ALL DEF CON ATTENDEES:

Everyone who comes to DEF CON is obliged to abide by DEF CON's photo and video guidelines/etiquette: let people know what you're doing, and be respectful.

The teams/film crews participating in this contest follow this etiquette, in part, by:

- being conspicuous, when they are filming in the DEF CON's convention areas,
- by wearing their bright orange, official, "TD Francis X-Hour Film Contest CREW" t-shirts
- letting bystanders know when they are actually filming by saying "ACTION" and "CUT", and other filmmaking sounding thingys and stuff
- not filming in designated no-camera areas
- obtaining permission when appropriate
- and being approachable and courteous to all.

Special Thanks to Jeff Moss, Kelly Brady, Alex Gravenstein, Frank Andrews, Rick Patyk, Dan Olbrych, Alex Hart, Darington Forbes, Algorythm, and DEF CON.

Cheers,

Thomas Waszak aka "Waz"

[www.xhourfilmcontest.com](http://www.xhourfilmcontest.com)

Twitter: @DEFCONFilmConte, @TDFXHourFilm

Instagram: @tdfxhour

[facebook.com/TDFXHourFilmContestAndFestival/](https://facebook.com/TDFXHourFilmContestAndFestival/)

DEF CON Forums: <https://forum.defcon.org/node/228307>

## D FRANCIS FILM CONTEST

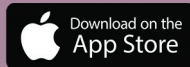
This could be the opportunity that's kicking open the door to your filmmaking greatness...

Assemble your team of 5 or less (director, producer, writer, camera/photography, editor) and make your cinematic marvel of short film here at DEF CON.

Actors and extras don't count towards the max 5, so

# HACKER TRACKER

Download the official DEF CON app! It contains all of the happenings of DEF CON. It is easy to use and updated as things change during the conference. It contains all of the maps and schedules so you can plan your best DEF CON experience.



## FORUM.DEFCON.ORG

No matter what part of the DEF CON universe you're interested in, you should start at the DEF CON Forums. With a forum account you can reach out to a local DEF CON group, help us plan future events or even chat with other hackers. DEF CON's heart is its community, and the community meets at the DEF CON Forums. Join us!



[HTTPS://PLAY.GOOGLE.COM/STORE/APPS/DEVELOPER?ID=DEF+CON+COMMUNICATIONS,+INC.](https://play.google.com/store/apps/developer?id=DEF+CON+COMMUNICATIONS,+INC.)



The screenshot shows the DEF CON Forums website interface. At the top is a navigation bar with links to forums, blogs, articles, defcon.org, media.defcon.org, defcongroups.org, infocon.org, reddit, and store. Below the navigation bar is a section titled 'Today's Posts' and 'Con Calendar'. The main content area is divided into two columns. The left column, titled 'ACTIVITY STREAM', shows a list of forum posts with details like topic, posts, and last post. The right column, titled 'Upcoming Events', shows a calendar of events for 2019, including DEF CON China 1.0, Packet Hacking Village CFP, and Creative Writing Short Story. Below the activity stream is a section titled 'DEF CON 27 Planning' with a list of sub-forums and their respective post counts.



**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 DEFCON.ORG. PRE-REGISTRATION WILL BE ONLINE AGAIN FOR DEF CON 28!**

	RED ROCK I	RED ROCK II	RED ROCK III	RED ROCK IV	RED ROCK V	RED ROCK VII	RED ROCK VIII
10:00-14:00	<p>From EK to DEK: Analyzing Document Exploit Kits</p> <p>Josh Reynolds</p>	<p>Hacking Medical Devices</p> <p>Jay Radcliffe</p>	<p>Hacking Wi-Fi for Beginners</p> <p>Alex Hammer</p>	<p>Learning to Hack Bluetooth Low Energy with BLE CTF</p> <p>Ryan Holeman</p>	<p>Pwning Serverless Applications</p> <p>Abhay Bargav</p>	<p>Constructing Kerberos Attacks with Delegation Primitives</p> <p>Elad Shamir</p>	<p>Introduction to Cryptographic Attacks (30)</p> <p>Matt Cheung</p>
14:30-18:30	<p>An Introduction to Deploying Red Team Infrastructure</p> <p>Troy Defty</p>	<p>Advanced Wireless Exploitation for Red Team and Blue Team</p> <p>Besim Altinok</p>	<p>Purple Team CTF</p> <p>Sam Bowne</p>	<p>Analysis 101 for Hackers and Incident Responders</p> <p>Kristy Westphal</p>	<p>Hacking the Android APK (40)</p> <p>Ben Hughes</p>	<p>Advanced Wireless Attacks Against Enterprise Networks</p> <p>solstice</p>	<p>Hacking Wifi</p> <p>Philippe Delteil</p>

	RED ROCK I	RED ROCK II	RED ROCK III	RED ROCK IV	RED ROCK V	RED ROCK VI	RED ROCK VII
10:00-14:00	Evil Mainframe Jr: Mainframe hacking from recon to privesc Phil Young	Malware Triage - Analyzing The Modern Malware Delivery Chain (35) Sergei Frankoff	Understanding and Analyzing Weaponized Carrier Files Ryan Chapman	Finding Vulnerabilities at Ecosystem-Scale Isaac Evans	Hacking ICS: From Open Source Tools to Custom Scripts Valerie Thomas	Hands on Adversarial Machine Learning Yacin Nadjji	Exploit Development for beginners Sam Bowne
14:30-18:30	Attacking Layer 2 Network Protocols Erik Dul	Breaking and Pwning Docker Containers and Kubernetes Clusters Madhu Akula	Reverse Engineering Android Apps Sam Bowne	Introduction to Sandbox Evasion and AMSI Bypasses Anthony Rose	Introduction to Reverse Engineering With Ghidra Wesley McGrew	Advanced Custom Network Protocol Fuzzing Joshua Pereyda	Defending environments and hunting malware with osquery (60) Guillaume Ross

	LAKE MEAD I	LAKE MEAD II	VALLEY OF FIRE I	VALLEY OF FIRE I
10:00-14:00	<p>Mind the Gap Between Attacking Windows and Mac: Breaking In and Out of Protected MacOS environments</p> <p>Richard Gold</p>	<p>Writing custom backdoor payloads using C#</p> <p>Mauricio Velazco</p>	<p>Red Teaming Techniques for Electronic Physical Security Systems (40)</p> <p>Valerie Thomas</p>	<p>Functional Programming for the Blue Team</p> <p>eigentourist</p>
14:30-18:30	<p>scapy_dojo_v_1 (26)</p> <p>Hugo Trovao</p>	<p>Modern Debugging^HWarfare with WinDbg Preview (20)</p> <p>Chris Alladoun</p>	<p>Hack to Basics - x86 Windows Based Buffer Overflows, an introduction to buffer overflows.(35)</p> <p>Dino Covotsos</p>	<p>Pentesting ICS T02</p> <p>Alexandrine TORRENTS</p>



# CFP REVIEW BOARD



## IN MEMORIAM: TERRENCE 'TUNA' GAREAU

THIS YEAR THE CFP REVIEW BOARD LOST ONE OF OUR OWN. TERRENCE "TUNA" GAREAU WAS AN AMAZING PERSON THAT LIT UP THE WORLD. HIS SPIRIT AND THIRST FOR LIFE WERE MATCHED ONLY BY HIS INTELLECT AND CARING HEART. TO MANY OF US, HE WAS OUR FRIEND, OUR CONFIDANT, OUR BROTHER, AND OUR HERO. WE WILL MISS HIM EVER SO DEARLY.

TUNA'S PASSING HAS LEFT A VOID INSIDE OUR HEARTS, BUT WE WILL CARRY HIS MEMORY WITH US ALWAYS AND REMEMBER THE JOY HE BOUGHT TO US ALL. TUNA, WE LOVE YOU AND WE MISS YOU, THANK YOU FOR BEING PART OF OUR LIVES EVEN IF IT WAS FOR SUCH A BRIEF TIME. WE ARE ALL BETTER PEOPLE HAVING KNOWN YOU.



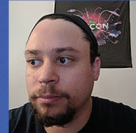
**JEFF MOSS**  
[AKA THE DARK TANGENT]  
TWITTER: @THEDARKTANGENT



**NIKITA KRONENBERG**  
[AKA NIKITA]  
DEF CON, DIRECTOR OF CONTENT & COORDINATION.  
WIFE & MOM, CHICKEN SOUP REPAIRWOMAN.  
SECURITYTRIBE. 🐼 🐼 🐼 SHELLACS 🐼  
INTO: HACKS 🐼 SNACKS 🐼 SHELLACS 🐼  
TWITTER: @NINJA  
AFFILIATIONS: THE TRIBE, DC509.2  
@WENATCHEEHACKERS



**ZOZ**  
[AKA THE HOFF, DR. WEIRD]  
INTERNATIONAL MAN OF MYSTERY  
AFFILIATIONS: BEEP OOK ORK AH AH



**ALEX**  
[AKA UNKNOWN]  
A JACK OF A FEW TRADES AND MASTER OF NONE  
AFFILIATIONS: UNKNOWN



**ASH**  
[AKA ASHMASTAFASH]  
MAKES SOME THINGS, BREAKS OTHER THINGS.  
ASHIRING COMBAT LOG FORT  
TWITTER: @ASHMASTAFASH  
AFFILIATIONS: STICH.IO



**PETE TEOH**  
[AKA CYBERSULU]  
DOES STUFF WITH CERTIFICATES (NOT GIFT CERTIFICATES), TRAVELS A LOT, AND HAS A DAY AGENCY.  
TWITTER: @CYBERSULU  
AFFILIATIONS: GOOGLE



**JOHN FULMER**  
[AKA DAKAHUNA]  
DAKAHUNA IS LIVING PROOF THAT ALCOHOL IS A PRESERVATIVE  
TWITTER: @DAKAHUNA8007  
AFFILIATIONS: THE TRIBE, NOVA HACKERS, SOX, SHELLBACK, GOAT LOCKER



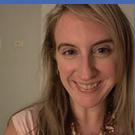
**DINO COVOTSOS**  
[AKA DINO, UNDISCLOSED]  
PROUD SOUTH AFRICAN HACKER, FOUNDER OF TELSPACE SYSTEMS AND PAYING IT FORWARD ONE DAY AT A TIME  
AFFILIATIONS: DC2711, TS



**SETH VAN OMMEN**  
[AKA BEAKER, SETHOPS]  
HI MOM!  
TWITTER: @SWORDOFMEN  
AFFILIATIONS: THE TRIBE, LHC



**CINDY JONES**  
[AKA SINDERZNAHSES, JUMPER ]  
SINDERZ IS AN UNABASHED MEAT-EATING, SIDE-EYE WINKING, VECROCRAPTOR WHO ENJOYS LATE EVENING WALKS ON THE BEACH  
TWITTER: @SINDERZNAHSES  
AFFILIATIONS: BOUNCY HOUSES AROUND THE WORLD



**MAGEN WU**  
[AKA TOTTEKOPHI]  
TOTTEKOPHI IS AN AI.. THAT OVERUSES EXCLAMATION POINTS IN TEXT-BASED COMMS AND THINKS THE PERFECT DATE IS APRIL 20TH.  
TWITTER: @MAGEN\_WU  
AFFILIATIONS: THE TRIBE, THE URBANE COLLECTIVE



**CHRIS GATES**  
[AKA CARNALOWNAGE]  
IT'S OK LIEBOW IF YOU ACTUALLY CARE  
TWITTER: @CARNALOWNAGE  
AFFILIATIONS: NOVA HACKERS



**SUGGY**  
[AKA NINJA PLAQUE]  
SUGGY IS THE TYPE OF KIRBYE PLAYER, THAT OTHER FORTNITE PLAYERS HATE, SCORING A COVERTED VICTORY ROYALE WITH ZERO KILLS BY HIDING UNDER A TREE  
TWITTER: @SUGGY  
AFFILIATIONS: YOU MIGHT FIND SUGGY AT THE DEF CON 4XSK OR HIDING UNDER A TREE



**GRANT**  
[AKA CLAVIGER, FISHSUPREME]  
YOLD.  
TWITTER: @FISHSUPREME



**DEAD ADDICT**  
[AKA EU]  
DEAD ADDICT ISNT A GOOD ENOUGH HUMAN BEING TO BE SELF-DEPRECATING IN HIS BIO



**HIGHWIZ**  
[AKA TOM, THE RAINBOW KING]  
HIGHWIZ IS THE FABLED MAN ON THE MOUNTAIN WHOM PEOPLE SEEK TO GAIN A TASTE OF HIS FORBIDDEN KNOWLEDGE  
TWITTER: @HIGHWIZ  
AFFILIATIONS: THE TRIBE, GH, DC, LHC



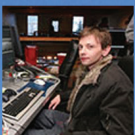
**JASON**  
[AKA WONK, ZOOMIE]  
ANGRY THAT EVERYONE IS PEEING IN THE POOL AND BRAGGING HOW BIG THEIR BLADDER IS  
TWITTER: @JASON\_HENLEY  
AFFILIATIONS: SDA, ATLANTIC COUNCIL



**MALWARE UNICORN**  
[AKA AMANDA ROUSSEAU]  
LINES REVERSING AND DEVELOPING MALWARE. BLUE TEAM TO RED TEAM CONVERT. PURSUES MAKING FREE CONTENT FOR THE COMMUNITY.  
TWITTER: @MALWAREUNICORN



**TIM MCGRUFFIN**  
[AKA MEDIC]  
TRIES TO KEEP HIS HEAD LOW. TAKES THINGS APART AND CAN SOMETIMES PUT THEM BACK TOGETHER.  
TWITTER: @TIMMCGRUFFIN  
AFFILIATIONS: THE TRIBE



**PWCRACK**  
[AKA PWCRACK]  
I BREAK ONE, 1-0-1-0-0. WITH THAT I COULD STEAL YOUR MONEY, YOUR SECRETS, YOUR SEXUAL FANTASIES, YOUR WHOLE LIFE. IN ANY COUNTRY, ANY TIME, ANY PLACE I WANT, WE MULTITASK LIKE YOU BREATHE. I COULDN'T THINK AS SLOW AS YOU IF I TRIED.  
TWITTER: @PWCRACK  
AFFILIATIONS: SPEAKER OPS, NOVA HACKERS, UNALLOCATED SPACE



**ERIN JACOBS**  
[AKA SECBARBIE]  
TO STRIVE ENDLESSLY TO STIR THE VENTURESOME SPIRIT THAT MOVES YOU TO FOLLOW A RAINBOW TO ITS END... AND THUS MAKE YOUR TRAVEL DREAMS COME TRUE  
TWITTER: @SECBARBIE  
AFFILIATIONS: SCOTCH AND BARRILES, 972 85, THE URBANE COLLECTIVE, HACKER CAMPERS



**SHAGGY**  
[AKA ALEX, SCRUFFY ]  
PENETRATES ALL NETWORKS EQUALLY AND DEEPLY  
TWITTER: @SHAGGYINCO  
AFFILIATIONS: THE TRIBE, SOX



**STEPHANIE**  
[AKA SNOW]  
ILS DEKAUFT ESSO, NIESAMOWITE! ПЕРШЫЙ ДЕ ЛА ПЮР ВИСЦІТЛІВЫЙ АРАСІНА КІОН ВЕДЗІКАНЕ Е ОІНЕ НІКОІМ ІНОДІТ ЭСО ПАРА КІНЦІ. КОММЕНТ КІНІТЕ ІЮ МОЗЛІВЕ ЕХТІ АСТЕПАТ А ЦІАКА СОМ ШКОЛА УЗЕРНІДЕ ОІНЕ ТІАК ПАСЕ ТІО ІЛЕ ЕСТЕ МІНОІМ СОЛІНОН ОІН ОІС СЕМЕСТЕР, КОНГРАТУЛАЗІОН, КОЛЕІНІ КІНО САРПЕ СЕІС ZERO CEMS СІРІР СІХ СІБІЕН QUATTRO DWA ПІРІВ  
TWITTER: @\_SNOW  
AFFILIATIONS: DC001, COOKIE MONSTAH CREW, HARBORSTRO, SOUX CREAM DONUTS, PARROT PACK, ALCATRAZ SWIM TEAM, DIRTY MIKE AND THE BOYS



**YAN**  
[AKA BCRYPT, AZUKI]  
WEB/BROWSER HACKER, CISO AT BRAVE SOFTWARE, FORMER STAFF TECHNOLOGIST AT EFF, OCCASIONALLY DJ AZUKI  
TWITTER: @BCRYPT  
AFFILIATIONS: UN MOM



**ZACK FASEL**  
[AKA ZFASEL ]  
WE KEEP MOVING FORWARD, OPENING NEW DOORS, AND DOING NEW THINGS, BECAUSE WE'RE CURIOSUS AND CURIOSITY KEEPS LEADING US DOWN NEW PATHS.  
TWITTER: @ZFASEL  
AFFILIATIONS: SCOTCH AND BARRILES, 972, 85, THE URBANE COLLECTIVE, UNLOCK CAMPERS



# PRESENTATIONS

Listed by Day, Time, Track

## THURSDAY

### EXPLOITING WINDOWS EXPLOIT MITIGATION FOR ROP EXPLOITS

Thursday at 10:00 in DC101, Paris Theatre  
45 minutes | Demo

**Omer Yair**

Endpoint Team Lead at Symantec

"A concept is a brick. It can be used to build a courthouse of reason. Or it can be thrown through the window."

\_ Gilles Deleuze

Ever since Smashing the Stack For Fun And Profit was published by Aleph One almost a quarter century ago the security world has completely changed the way it defends exploitation. Canary stack, DEP, ASLR, CFI and various other mitigation techniques were developed to address various exploit techniques. Yet, ROP remains a prominent practice employed by many exploits even today.

ROP is the most common exploitation method for attackers to mutate memory bugs on target process into malicious executable code. "Next Gen" endpoint security products try to address ROP and other exploitation methods. Windows embraces many mitigation techniques as well. However, these mitigation features such as CFG can in fact be leveraged and increase ROP's attack surface and allow it to even bypass exploit protections!

If you are intrigued by ROP, want to learn about methods in Windows that protect against ROP and how to bypass them - this talk is for you! On top of that a novel method of bypassing ROP mitigation of most products will also be revealed.

### BREAKING GOOGLE HOME: EXPLOIT IT WITH SQLITE (MAGELLAN)

Thursday at 11:00 in DC101, Paris Theatre  
45 minutes | Demo, Exploit

**Wenxiang Qian**

Senior security researcher at Tencent Blade Team

**YuXiang Li**

Senior security researcher at Tencent Blade Team

**HuiYu Wu**

Senior security researcher at Tencent Blade Team

Over the past years, our team has used several new approaches to identify multiple critical vulnerabilities in SQLite and Curl, two of the most widely used basic software libraries. These two sets of vulnerabilities, which we named "Magellan" and "Dias" respectively, affect many devices and software. We exploited these vulnerabilities to break into some of the most popular Internet of things devices, such as Google Home with

Chrome. We also exploited them on one of the most widely used Web server (Apache+PHP) and one of the most commonly used developer tool (Git).

In this presentation, we will share how we try to crack the Google Home from both hardware and software aspects, get and analyze the newest firmware, solve the problem, and introduce new methods to discover vulnerabilities in SQLite and Curl through Fuzz and manual auditing. Through these methods, we found "Magellan", a set of three heap buffer overflow and heap data disclosure vulnerabilities in SQLite ( CVE-2018-20346, CVE-2018-20505 CVE-2018-20506 ) We also found "Dias", two remote memory leak and stack buffer overflow vulnerabilities in Curl ( CVE-2018-16890 and CVE-2019-3822 ). Considering the fact that these vulnerabilities affect many systems and software, we have issued a vulnerability alert to notify the vulnerable vendor to fix it.

We will disclose the details of "Magellan" and "Dias" for the first time and highlight some of our new vulnerability exploitation techniques. In the first part, we will introduce the results of our analysis on hardware, how to get the newest firmware from simulating an update request, and attack surface of Google Home. We will show how to use Magellan to complete the remote exploit of Google Home, we will also give a briefing talk about how to use Dias to complete the remote attack on Apache+PHP and Git. Finally, we will summarize our research and provide some security development advice to the basic software library developers.

### ARE QUANTUM COMPUTERS REALLY A THREAT TO CRYPTOGRAPHY? A PRACTICAL OVERVIEW OF CURRENT STATE-OF-THE-ART TECHNIQUES WITH SOME INTERESTING SURPRISES

Thursday at 12:00 in DC101, Paris Theatre  
45 minutes | Demo

**Andreas Baumhof**

Vice President Quantum Technologies, QuintessenceLabs Inc.

Shor's Algorithm for factoring integer numbers is the big threat to cryptography (RSA/ECC) as it reduces the complexity from exponential to polynomial, which means a Quantum Computer can reduce the time to crack RSA-2048 to a mere 10 seconds. However current noisy NISQ type quantum computers are very limited to something like 16 bit RSA keys. And the quality of the current qubits is so bad that error-correction comes at a massive cost of at least 100 times the amount of qubits.

While the world is pre-occupied whether we have universal quantum computers big enough for Shor's algorithm, Quantum Annealing is stealing the show with having factored a 20-bit number just in January this year using 97 qubits. And these qubits are actually good enough to factor bigger numbers. If we assume a linear scalability, we'd "only" need around 10,000 qubits to factor a 2048bit RSA key. D-Wave announced a quantum computer with 5,640 qubits, so that puts it within reach soon.

So, could Quantum Annealing be more of a threat



# PRESENTATIONS

to cryptography than Shor's algorithm on universal quantum computers? How do these algorithms work? How do they achieve a polynomial complexity to what traditional computers need exponential time? What impact will this have on the competition from NIST for the design of post-quantum-cryptography algorithms?

## INTRO TO EMBEDDED HACKING—HOW YOU TOO CAN FIND A DECADE OLD BUG IN WIDELY DEPLOYED DEVICES. (REDACTED) DESKPHONES, A CASE STUDY.

Thursday at 13:00 in DC101, Paris Theatre  
45 minutes | Demo, Exploit

**Philippe Lautheret**

Senior Security Researcher @ McAfee Advanced Threat Research

From small business to large enterprise, VOIP phones can be found on nearly every desk. But how secure are they? What if your phone was spying on every conversation you have? This talk is an introduction to hardware hacking and as a case study I'll use the [REDACTED] Deskphone, a device frequently deployed in corporate environments. I'll use it to introduce the tools and methodology needed to answer these questions.

During this talk, attendees will get a close up look at the operations of a hardware hacker, including ARM disassembly, firmware extraction using binwalk, micro-soldering to patch an EEPROM and get a root shell over UART, and ultimately uncover an already known decade-old bug that somehow remained unnoticed in the device's firmware.

Beyond the case study I will also address alternative tactics; some did not work, others may have but were not the lowest-hanging fruit. When it comes to hardware hacking, the process is as important as the result; knowing that there are multiple ways to reach the end goal helps researchers remain confident when hurdles arise. After the talk, attendees will have an increased distrust towards always-on devices; however, they will have the background knowledge to investigate the products and systems they encounter daily.

## WEB2OWN: ATTACKING DESKTOP APPS FROM WEB SECURITY'S PERSPECTIVE

Thursday at 14:00 in DC101, Paris Theatre  
45 minutes

**Junyu Zhou**

Security Researcher in Tencent Security Xuanwu Lab

**Ce Qin**

Security Researcher in Tencent Security Xuanwu Lab

**Jianing Wang**

Security Researcher in Tencent Security Xuanwu Lab

People are always talking about binary vulnerabilities when attacking desktop applications. Memory corruptions are always costly to find. Meanwhile, mitigations introduced by operating systems make them

harder to be exploited. More and more applications are using hybrid technologies, so we can try web security tricks to pwn them reliably with less effort.

Our presentation will summarize attack surfaces and methods to find security issues in desktop applications. In particular, we will explicate some real-world cases, such as chaining multiple vulnerabilities (information leaking, CSP bypass, opened debugging port) to achieve RCE in a specialized IDE, sensitive file leaking in famous editors, privileged APIs abusing in many IM applications and so on. During our research, we find some issues actually reside in popular libraries. These flaws may affect more applications than we will demonstrate in this talk.

Web security knowledge is usually unfamiliar to desktop application developers. Attacking desktop apps using web security tricks is a non-competitive "blue ocean". Our presentation will focus on many design misconceptions and implementation mistakes in desktop applications. By sharing these representative lessons, we hope to help desktop application developers improve the security of their products.

## DEF CON 101 PANEL

Thursday at 15:00 in DC101, Paris Theatre  
105 minutes

**Highwiz**

**Nikita**

**Will**

**n00bz**

**Shaggy**

**SecBarbie**

**Tottenkoph**

The DEF CON 101 Panel is the place to go to learn about the many facets of DEF CON and to begin your DEF CONian Adventure. The idea is to help attendees get the best experience out of DEF CON (and also tell them how to survive the weekend!). It is 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, you can stick around for the n00b party after the panel and get your handle then!



# THURSDAY / FRIDAY

## FRIDAY

### BEHIND THE SCENES OF THE DEF CON 27 BADGE

Friday at 10:00 in Track 1  
45 minutes | Tool

#### Joe Grand (Kingpin)

Incorporating natural elements, complex fabrication techniques, and components rarely seen by the outside world, the DEF CON 27 Badge brings our community together through Technology's Promise. Join DEF CON's original electronic badge designer Joe Grand on a behind-the-scenes journey of this year's development process and the challenges, risks, and adventures he faced along the way.

### HACKING CONGRESS: THE ENEMY OF MY ENEMY IS MY FRIEND

Friday at 10:00 in Track 2  
45 minutes

#### Former Rep. Jane Harman

President, The Wilson Center, Former Rep. (D-CA), aka Surfer Jane

#### Rep. James Langevin

(D-RI)

#### Jen Ellis

Director of Public Affairs, Rapid 7

#### Cris Thomas

Director, X-Force Red Team, IBM, aka Space Rogue

#### Rep. Ted Lieu

(D-CA)

A SIMULATED crisis is unfolding on a national scale, based loosely on the NotPetya attack of 2017. Triggered by a yet-unknown adversary, what started as an isolated technical issue has quickly escalated into a society-wide event affecting millions of citizens, several industries, and spanning government jurisdictions. Who is in charge, how do they cooperate with others, and how do they make decisions? The Wilson Center, Hewlett Foundation and I Am The Calvary are teaming up to bring public policymakers together with security researchers and others to discover how our nation might respond to a wide-scale "cyber crisis". Work in tandem with sitting Members of Congress to understand what levers of power Congress yields and how Members can address policy gaps in the future.

### BEHIND THE SCENES: THE INDUSTRY OF SOCIAL MEDIA MANIPULATION DRIVEN BY MALWARE

Friday at 10:00 in Track 3  
45 minutes

#### Olivier Bilodeau

Cybersecurity Research Lead at GoSecure

#### Masarah Paquet-Clouston

Cybersecurity Researcher at GoSecure

This talk is the grand finale of a four-year long investigation that started with analyzing an IoT botnet, to discovering the structured industry that exists behind social media manipulation (SMM). SMM is the deliberate act of paying for popularity with followers or activity on social media.

Adopting a bottom-up approach, the thorough methodology undertook to study the botnet will be presented: from building honeypots, infecting them with malware and conducting a man-in-the-middle-attack on the honeypots' traffic to access the decrypted HTTPS content between the C&Cs and social networks. Then, the various investigative paths taken to analyze this large data set, leading to the discovery of industry actors involved in the supply chain of social media manipulation, will be presented. These investigative paths include traffic analysis, various OSINT approaches to reveal and understand actors, reverse-engineering the software that automates the use and creation of fake accounts, forum investigations, and qualitative profiling. All actors involved in the industry will be mapped, from malware authors, to reseller panels, and customers of fake popularity.

The potential profitability of the industry will then be discussed, as well as the revenue division in the chain, demonstrating that the ones making the highest revenue per fake follower sold are not the malware authors, but rather those at the end of the chain.

### DUPLICATING RESTRICTED MECHANICAL KEYS

Friday at 10:00 in Track 4  
45 minutes | Exploit

#### Bill Graydon

President and Principal, Physical Security Analytics

#### Robert Graydon

Principal, GGR Security

Secure facilities in North America use lock systems like Medeco, Abloy, Assa and Mul-T-Lock partly to resist lock picking, but also to prevent the duplication and creation of unauthorised keys. Places such as the White House and the Canadian Parliament buildings go so far as to use a key profile exclusive to that facility to ensure that no-one is able to obtain key blanks on which to make a copy. However, there are tens of thousands of unrestricted key blank profiles in existence - many match very closely to these restricted key blanks, and can be used instead of the real blanks to cut keys on. Moreover, keys are just pieces of metal - we will present numerous practical techniques to create restricted keys without authorisation - including

# PRESENTATIONS

new attacks on Medeco, Mul-T-Lock and Abloy key control systems. We will touch on all aspects of key control, including patents and interactive elements, and discuss how to defeat them and how facility managers can fight back against these attacks.

## DON'T RED-TEAM AI LIKE A CHUMP

Friday at 11:00 in Track 1  
45 minutes | Demo, Tool

**Ariel Herbert-Voss**

PhD student, Harvard University

AI needs no introduction as one of the most overhyped technical fields in the last decade. The subsequent hysteria around building AI-based systems has also made them a tasty target for folks looking to cause major mischief. However, most of the popular proposed attacks specifically targeting AI systems focus on the algorithm rather than the system in which the algorithm is deployed. We'll begin by talking about why this threat model doesn't hold up in realistic scenarios, using facial detection and self-driving cars as primary examples. We will also learn how to more effectively red-team AI systems by considering the data processing pipeline as the primary target.

## THE TOR CENSORSHIP ARMS RACE: THE NEXT CHAPTER

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

**Roger Dingledine**

The Tor Project

Tor is a free-software anonymizing network that helps people around the world use the Internet in safety. But who cares how good Tor's privacy is, if your government prevents you from reaching the Tor network?

In the beginning, some countries filtered torproject.org by DNS (so we made website mirrors and an email autoresponder for downloading Tor), and then some countries blocked Tor relays by IP address (so we developed bridges, which are essentially unlisted relays), and then some countries blocked Tor traffic by Deep Packet Inspection (so we developed pluggable transports to transform Tor flows into benign-looking traffic).

Then things got weird, with China's nationwide active probing infrastructure to enumerate bridges, with Amazon rolling over to Russia's threats when Telegram used "domain fronting" to get around blocking, with Turkey blocking Tor traffic by DPI in more subtle ways, with Venezuela and Ethiopia and Iran trying new tricks, and more.

In this talk I'll get you up to speed on all the ways governments have tried to block Tor, walk through our upcoming steps to stay ahead of the arms race, and give you some new—easier—ways that let you help censored users reach the internet safely.

## ALL THE 4G MODULES COULD BE HACKED

Friday at 11:00 in Track 3  
45 minutes | Exploit

**XiaoHuiHui**

Senior Security Researcher, Baidu

**Ye Zhang**

Security Researcher, Baidu

**ZhengHuang**

Leader of Baidu Security Lab X-Team, Baidu

Nowadays more and more 4G modules are built into IoT devices around the world, such as vending machines, car entertainment systems, laptops, advertising screens, and urban cameras etc. But no one has conducted a comprehensive security research on the 4G modules. We carried out this initiative and tested all the major brand 4G modules in the market (more than 15 different types). The results show all of them have similar vulnerabilities, including remote access with weak passwords, command injection of AT Command/listening services, OTA upgrade spoofing, command injection by SMS, and web vulnerability. Through these vulnerabilities we were able to get to the shell of these devices. In addition to using wifi to exploit these vulnerabilities, we created a new way to attack through fake base station system, triggered by accessing the intranet of cellular network, and successfully run remote command execution without any requisites. In this talk, we will first give an overview on the hardware structure of these modules. Then we will present the specific methods we use in vulnerability probe. In the final section we will demonstrate how to use these vulnerabilities to attack car entertainment systems of various brands and get remote control of cars.

## EVIL EBPF IN-DEPTH: PRACTICAL ABUSES OF AN IN-KERNEL BYTECODE RUNTIME

Friday at 11:00 in Track 4  
45 minutes | Demo, Exploit

**Jeff Dileo**

Research Director, NCC Group

eBPF (or "extended" Berkeley Packet Filter) is a bytecode instruction set and virtual machine used as a safe computing environment within the Linux kernel to perform arbitrary programmatic actions. It is a redesign of Linux's original in-kernel BPF bytecode VM used to power features like tcpdump filters. eBPF has an entirely different set of capabilities and instructions, with its primary goal being to serve as a JIT-able virtual machine instruction set that can be targeted by compilers of a memory-safe "restricted C" language. In the Linux kernel, it is actively being applied to anything and everything to provide performant programmatic capabilities to userland that extend traditionally kernel-based functionality.

In this exploit development focused talk, we will first introduce eBPF and discuss several nefarious techniques enabled by the technology. As we do so, we will cover the respective sets of APIs, file descriptor types, and other eBPF machinery that enable such techniques,



building up from various forms of hidden IPC channels to full-fledged rootkits. Within this talk, we will walk through the implementations of the techniques we discuss so that attendees will walk away with the knowledge of how to implement their own variants. Along the way we will discuss novel container breakout techniques and interesting “dual-purpose” eBPF features that enable the development of mutative syscall hooks that work for processes that work for processes already attached by a debugger. Finally, we will provide insight on how defenders should begin to attempt to detect and recover from such abuses, when possible at all.

This presentation significantly extends on work we first presented at 35C3, which focused more heavily on the underlying aspects of general eBPF-based kernel tracing. In contrast, this talk will demo new techniques and include substantially improved versions of techniques presented previously as proofs-of-concept.

## PROCESS INJECTION TECHNIQUES - GOTTA CATCH THEM ALL

Friday at 12:00 in Track 1  
45 minutes | Tool

**Itzik Kotler**

Co-Founder & CTO at SafeBreach

**Amit Klein**

VP Security Research at SafeBreach

When it comes to process injection in Windows, there are only 6-7 fundamental techniques, right? Wrong. In this talk, we provide the most comprehensive to-date “Windows process injection” collection of techniques. We focus on Windows 10 x64, and on injections from running 64-bit medium integrity process to another running 64-bit medium integrity process, without privilege elevation. We pay special attention to the new Windows protection technologies, e.g. CFG and CIG. We differentiate between memory write primitives and execution techniques, and discuss memory allocation strategies. Our collection is curated, analyzed, tabulated, with straight-forward, research-grade PoCs. We tested each technique against Windows 10 x64 with and without protections, and we report on the requirements, limitations, and quirks of each technique. And of course—no decent DEF CON presentation is complete without new attacks. We describe a new memory writing primitive which is CFG-agnostic. We describe a new “stack bombing” execution method (based on the memory write primitive above) that is inherently safe (even though overwriting the stack is a-priori a dangerous and destabilizing action). Finally, we release a library of all write primitives and execution methods, so users can generate “tailor-made” process injections.

## PHREAKING ELEVATORS

Friday at 12:00 in Track 2  
45 minutes | Demo

**WillC**

This is a comprehensive dive into the current emergency phones with an in-depth look at the phones used in elevators. This talk will provide unique insight into a topic that hasn't been covered before: Elevator Phones. During this talk, I will discuss the commonality between elevator phone brands. I will cover a new, never before released, set of default passwords these system use. I will show a tool kit and how to use it to access elevator phones locally, as well as remotely. In addition, I will show how to reprogram a phone, how to make the elevator state its location, and how to alert the passenger that help is on the way. Finally, I will demonstrate some attacks, including how you can use elevator phones as listening devices to silently listen to conversations of people inside an elevator. I'm WillC, your elevator operator, let's go for a ride!

## INFILTRATING CORPORATE INTRANET LIKE NSA \_ PRE-AUTH RCE ON LEADING SSL VPNS

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

**Orange Tsai**

Principal Security Researcher from DEVCORE, Member of HITCON(Hacks in Taiwan Conference), Member of CHROOT Security Group, Captain of HITCON CTF team

**Meh Chang**

Security Researcher from DEVCORE, Member of HITCON CTF team

Computer security is now a public policy issue. Election security, blockchain, “going dark,” the vulnerabilities equities debate, IoT safety, data privacy, algorithmic security and fairness, critical infrastructure: these are all important public policy issues with a strong Internet security component. But while an understanding of the technology involved is fundamental to crafting good policy, there is little involvement of technologists in policy discussions. This is not sustainable. We need public-interest technologists: people from our fields helping craft policy, and working to provide security to agencies and groups working in the broader public interest. We need these people in government, at NGOs, teaching at universities, as part of the press, and inside private companies. This is increasingly critical to both public safety and overall social welfare. This talk both describes the current state of public-interest technology, and offers a way forward for us individually and collectively for our field. The defining policy question of the Internet age is this: How much of our lives should be governed by technology, and under what terms? We need to be involved in that debate. SSL VPNs protect corporate assets from Internet exposure, but what if SSL VPNs themselves are vulnerable? They're exposed to the Internet, trusted to reliably guard the only way to intranet. However, we found pre-auth RCEs on multiple leading SSL VPNs, used by nearly half of the Fortune 500 companies and many government organizations. To make things worse, a “magic” backdoor was found to allow changing any

# PRESENTATIONS

user's password with no credentials required! To show how bad things can go, we will demonstrate gaining root shell from the only exposed HTTPS port, covertly weaponizing the server against their owner, and abusing a hidden feature to take over all VPN clients!

In such complicated closed-source systems, gaining root shell from outside the box certainly ain't easy. It takes advanced web and binary exploitation techniques to struggle for a way to root shell, which involves abusing defects in web architectures, hard-core Apache jemalloc exploitation and more. We will cover every detail of all the dirty tricks, crazy bug chains, and the built-in backdoor. After gaining root shell into the box, we then elaborate on post exploitation and how we hack back the clients. In addition, we will share the attack vectors against SSL VPNs to kick start researches on similar targets. On the other hand, from our previous experience, we derive general hardening actions that mitigate not only all the above attacks, but any other potential 0days.

In summary, we disclose practical attacks capable of compromising millions of targets, including tech giants and many industry leaders. These techniques and methodologies are published in the hope that it can inspire more security researchers to think out-of-the-box; enterprises can apply immediate mitigation, and realize that SSL VPN is not merely Virtual Private Network, but also a "Vulnerable Point of your Network".

## API-INDUCED SSRF: HOW APPLE PAY SCATTERED VULNERABILITIES ACROSS THE WEB

Friday at 12:00 in Track 4  
45 minutes | Demo, Exploit

**Joshua Maddux**

Security Researcher / Software Engineer, PKC Security

The 2016 WWDC saw the dawn of Apple Pay Web, an API that lets websites embed an Apple Pay button within their web-facing stores. Supporting it required a complex request flow, complete with client certificates and a custom session server. This proved detrimental, since Apple failed to caution against important side effects of taking in untrusted URLs. As a result, many new SSRF vulnerabilities entered the world. Worse yet, while they were exploitable and discoverable in similar ways, they were spread across distinct codebases in several programming languages, so could not be patched in any generic way.

Apple is not alone - in the process of gluing the web together, Twilio, Salesforce, and others have all created similarly broad attack surfaces. When companies fail to take an honest, empathetic look at how clients will use a product, they shove along hidden security burdens. Those who integrate with an API have less context than those who create it, so are in a worse position to recognize these risks.

Engineers have been talking about defensive programming for decades, but top companies still have trouble practicing it. In this talk we explore these mistakes with demos of affected software, and introduce a powerful model for finding broad classes of bugs.

## HACKPAC: HACKING POINTER AUTHENTICATION IN IOS USER SPACE

Friday at 13:00 in Track 1  
45 minutes | Demo, Tool, Exploit

**Xiaolong Bai  
Min (Spark) Zheng**

Pointer Authentication (in short, PAuth) is the latest security mechanism in iOS. It is proposed to protect the integrity of pointers with hardware-assisted encryption, thus eliminating the threats of code-reuse attacks. In PAuth, a cryptographic signature called PAC is calculated from a pointer value and inserted into the pointer. When the pointer is about to be used, the PAC is extracted and verified whether it is consistent with the original pointer value. In this way, PAuth is able to ensure that the pointers are not tampered. iOS deployed PAuth in user-space system services, protecting pointers that may affect the control flow and preventing code-reuse attacks like ROP and JOP.

However, in our study, we found that a fatal flaw in the implementation of iOS PAuth makes user-space system services still vulnerable to code-reuse attacks. The flaw is: iOS uses the same signing key in different user-space processes. This flaw allows a signed pointer from a malicious process can be correctly verified in a system service, thus making it possible to launch JOP. In this talk, we will explain how we found the flaw and why it is inevitable. In advance, we will demonstrate how to leverage this flaw and launch JOP attacks in a PAuth-protected system service. Also, we will propose a new tool, PAC-gadget, to automatically find JOP gadgets in PAuth-protected binaries.

## HVACKING: UNDERSTAND THE DIFFERENCE BETWEEN SECURITY AND REALITY!

Friday at 13:00 in Track 2  
45 minutes | Demo

**Douglas McKee**

Senior Security Researcher, McAfee Advanced Threat Research

**Mark Bereza**

Security Researcher, McAfee Advanced Threat Research

Like most modern devices, building controllers have increasingly become network connected, exposing them to a wider range of threats. If malicious actors could manipulate access control systems, boiler rooms, or temperature control for critical industrial systems, the potential for catastrophic damage is extreme.

McAfee's ATR team has discovered a 0-day vulnerability in a major building controller. This controller is a fully programmable native BACnet® device designed to manage a wide range of building systems. By modifying BACnet broadcast traffic, a buffer overflow can be leveraged into a write-what-where (WWW) condition. This WWW leads to execution control, providing the attacker with a root shell and complete control over the device remotely. Because this attack vector is through BACnet broadcast traffic, there is no authentication mechanism for the target device, allowing anyone on the same



network to communicate with it directly and exploit the vulnerability without authentication. Currently, there are over 500 of these devices connected to the internet running in BACnet/IP Broadcast Management Device (BBMD) mode. Utilizing this mode, broadcast traffic can travel over the internet, increasing the potentially devastating impact of this vulnerability.

This presentation will include a deep technical analysis of the vulnerability discovery process and demos illustrating an attack in a critical scenario. Finally, we will discuss the steps taken by the vendor to patch this vulnerability and demonstrate its effectiveness.

## NO MAS--HOW ONE SIDE-CHANNEL FLAW OPENS ATM, PHARMACIES AND GOVERNMENT SECRETS UP TO ATTACK

Friday at 13:00 in Track 3  
45 minutes | Demo, Exploit

phar  
ioactive

Hacking 'high security' electronic locks has become a bit of a hobby, but what if you identify an unpatchable design pattern that unlocks buckets of cash and government secrets? How long do wait before telling 'people'? let's talk about how these locks are designed, where they fail and we can rip this band-aid off together.

## MORE KEYS THAN A PIANO: FINDING SECRETS IN PUBLICLY EXPOSED EBS VOLUMES

Friday at 13:00 in Track 4  
45 minutes | Demo, Tool

xBen "benmap" Morris

Security Associate, Bishop Fox

Did you know that Elastic Block Storage (Amazon EBS) has a "public" mode that makes your virtual hard disk available to anyone on the internet? Apparently hundreds of thousands of others didn't either, because they're out there exposing secrets for everyone to see.

I tore apart the petabytes of data for you and have some dirty laundry to air: encryption keys, passwords, authentication tokens, PII, you name it and it's here. Whole (virtual) hard drives to live sites and apps, just sitting there for anyone to read. So much data in fact that I had to invent a custom system to process it all.

There's a massive Wall of Sheep out there on the internet, and you might not have even noticed that you're on it. Actually, you should stop reading and go check that out right now.

## HARNESSING WEAPONS OF MAC DESTRUCTION

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

Patrick Wardle

Chief Research Officer, Digma Security

Whenever a new Mac malware specimen is uncovered, it provides a unique insight into the offensive Mac capabilities of hackers or nation-state adversaries. Better yet, such discoveries provide fully-functional capabilities that may be weaponized for our own surreptitious purposes! I mean, life is short, why write your own?

We'll begin this talk by discussing the methodology of subverting existing malware for "personal use", highlighting both the challenges and benefits of such an approach.

Next, we'll walk-thru the weaponization of various Mac malware specimens, including an interactive backdoor, a file-exfiltration implant, ransomware, and yes, even adware. Customizations include various runtime binary modifications that will coerce such malware to accept tasking from our own C&C servers, and/or automatically perform actions on our behalf.

Of course, in their pristine state, such samples are currently detected by AV products. As such we'll also walk-thru subtle modifications that will ensure our modified tools remains undetected by traditional detection approaches.

In conclusion, we'll highlight novel heuristic methods that can generically detect such threats to ensure Mac users remain protected even from such weaponized threats.

## ARE YOUR CHILD'S RECORDS AT RISK? THE CURRENT STATE OF SCHOOL INFOSEC

Friday at 14:00 in Track 2  
45 minutes

Bill Demirkapi

Independent Security Researcher

From credit reporting agencies to hotel enterprises, major data breaches happen daily. However, when was the last time we considered the data security of children and middle-level education students? The infosec community spends so much time thinking about enterprise security and user privacy, but who looks after those who can't defend themselves? Unknown to most, there are only just a handful of major educational software providers—and flaws in any of them can lead to massive holes which expose the confidential information of our rising generation, this speaker included. Additionally, while many dismiss educational data as "just containing grades", the reality is that these systems store extremely sensitive information from religious beliefs, health and vaccine-related data, to even information about parental abuse and drug use in the family.

This talk will cover never-before-seen research into the handful of prominent educational software companies, the vulnerabilities that were found, the thousands

# PRESENTATIONS

of schools and millions of students affected, and the personal fallout of such research. Vulnerabilities discussed will range from blind SQL injection to leaked credentials for the entire kingdom. If a high school student can compromise the data of over 5 million students and teachers, what can APT do?

## HOW DEEP LEARNING IS REVOLUTIONIZING SIDE-CHANNEL CRYPTANALYSIS

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

**Elie Bursztein**

Google

**Jean Michel Picod**

Google

This talk explores how AI is revolutionizing hardware side-channel attacks and what this new wave of attacks mean for the future of hardware cryptography. Based on the lessons learned while successfully attacking many hardware AES implementations using deep-learning this talk discuss why those attacks are fundamentally more efficient and details how to conduct them in practice.

## PRACTICAL KEY SEARCH ATTACKS AGAINST MODERN SYMMETRIC CIPHERS

Friday at 14:00 in Track 4  
45 minutes | Demo

**Daniel “ufurnace” Crowley**

Research Baron, X-Force Red

**Daniel Pagan**

Student, Georgia Tech

In theory, brute force key recovery attacks against modern ciphers like AES should be impractical with the current state of computer hardware. It's often said that recovering an AES key should take longer than the remainder of the life of the sun. However, this assumes that keys are chosen properly, and that there is no way to determine whether a key is the correct one after a candidate key is used to decrypt a captured ciphertext. In practice, these conditions do not always hold. In much the same way that hash functions are impossible to reverse but hash cracking is still a practical attack, in the real world it is often possible to perform practical key search attacks. In this talk, we will discuss the common mistakes and common conditions that allow for practical brute force recovery of keys for modern block ciphers such as AES. We will also discuss optimizations to speed up key search efforts, and present our FOSS tool, which implements our approach.

## MOSE: USING CONFIGURATION MANAGEMENT FOR EVIL

Friday at 15:00 in Track 1  
45 minutes | Demo, Tool

**Jayson Grace**

Penetration Tester, Splunk

Configuration Management (CM) tools are used to provision systems in a uniform manner. CM servers are prime targets for exploitation because they are connected with key machines. The tools themselves are powerful from a security standpoint: they allow an attacker to run commands on any and every connected system. Unfortunately, many security professionals do not have CM experience, which prevents them from using these tools effectively. MOSE empowers the user to weaponize an organization's CM tools without having to worry about implementation-specific details.

MOSE first creates a binary based on user input. Once transferred to the CM server and run, this binary dynamically generates code that carries out the desired malicious behavior on specified systems. This behavior can include running arbitrary system commands, creating or deleting files, and introducing backdoors. MOSE puts the generated code in the proper place so that all targeted systems will run it on their next check-in with the server, removing the need for the user to integrate it manually.

CM tools are a powerful resource, but they have a barrier to entry. MOSE aims to remove this barrier and make post exploitation more approachable by providing a tool to translate the attacker's desired task into commands executable by the CM infrastructure.

## CHANGE THE WORLD, CDC STYLE: COW TIPS FROM THE FIRST 35 YEARS

Friday at 15:00 in Track 2  
45 minutes

**Joseph Menn**

Author, *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World* (PublicAffairs, June 2019)

**Peiter Mudge Zatkow**

**Chris Dildog Rioux**

**Deth Vegetable**

**Omega**

The Cult of the Dead Cow changed the culture of the entire security industry, the attitude of companies who had ignored risks, and even how the feds dealt with hackers. In this session, four key figures from the group's first 35 years will cover their greatest hits and screw-ups, highlighting the lessons for other hackers out to make a difference.

They will be questioned by Joseph Menn, whose new book on the group shows how it evolved from a network of bulletin board operators to the standard-bearers of hacker culture. cDc Minister of Propaganda Deth Vegetable and long serving text-file editor Omega will appear for the first time under their real names, covering the group's



formative years and how it handled such recent controversies as WikiLeaks, neo-Nazis, and the presidential candidacy of cDc alum Beto O'Rourke.

cDc tech luminaries Zatko and Rioux will discuss the release of Back Orifice at Def Con in 1998, which allowed non-hackers to hijack Windows machines, drawing worldwide attention to the insecurity of Microsoft's operating system, and Rioux's pathbreaking sequel, Back Orifice 2K, which prompted Microsoft to hire hackers as security consultants, including those from Zatko and Rioux's @stake. Zatko will share insights from leading inside the government, where he ran cybersecurity grantmaking at DARPA, the people who brought you the internet. And Rioux will explain what's possible in the private sector, where he co-founded unicorn Veracode, which dramatically improved code review by major software buyers.

## 100 SECONDS OF SOLITUDE: DEFEATING CISCO TRUST ANCHOR WITH FPGA BITSTREAM SHENANIGANS

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

**Jatin Kataria**

Principal Scientist, Red Balloon Security

**Rick Housley**

Research Scientist, Red Balloon Security

**Ang Cui**

Chief Scientist, Red Balloon Security

First commercially introduced in 2013, Cisco Trust Anchor module (TAm) is a proprietary hardware security module that is used in a wide range of Cisco products, including enterprise routers, switches and firewalls. TAm is the foundational root of trust that underpins all other Cisco security and trustworthy computing mechanisms in such devices. We disclose two 0-day vulnerabilities and show a remotely exploitable attack chain that reliably bypasses Cisco Trust Anchor. We present an in-depth analysis of the TAm, from both theoretical and applied perspectives. We present a series of architectural and practical flaws of TAm, describe theoretical methods of attack against such flaws. Next, we enumerate limitations in current state-of-the-art offensive capabilities that made the design of TAm seem secure.

Using Cisco 1001-X series of Trust Anchor enabled routers as a demonstrative platform, we present a detailed analysis of a current implementation of TAm, including results obtained through hardware reverse engineering, Trust Anchor FPGA bitstream analysis, and the reverse engineering of numerous Cisco trustworthy computing mechanisms that depend on TAm. Finally, we present two 0-day vulnerabilities within Cisco IOS and TAm and demonstrate a remotely exploitable attack chain that results in persistent compromise of an up-to-date Cisco router. We discuss the implementation of our TAm bypass, which involves novel methods of reliably manipulating FPGA functionality through bitstream analysis and modification while circumventing the need to perform RTL reconstruction. The use of our methods of manipulation creates numerous

possibilities in the exploitation of embedded systems that use FPGAs. While this presentation focuses on the use of our FPGA manipulation techniques in the context of Cisco Trust Anchor, we briefly discuss other uses of our bitstream modification techniques.

## RELAYING CREDENTIALS HAS NEVER BEEN EASIER: HOW TO EASILY BYPASS THE LATEST NTLM RELAY MITIGATIONS

Friday at 15:00 in Track 4  
45 minutes | Demo, Tool, Exploit

**Marina Simakov**

Senior Security Researcher @Preempt

**Yaron Zinar**

Senior Security Researcher Lead @Preempt

Active Directory has always been a popular target for attackers, with a constant rise in attack tools attempting to compromise and abuse the main secrets storage of the organization. One of the weakest spots in Active Directory environments lies in the design of one of the oldest authentication protocols—NTLM, which is a constant source of newly discovered vulnerabilities. From CVE-2015-0005, to the recent LDAP Relay vulnerability, it is clear why this protocol is one of the attackers' favorites.

Although there are offered mitigations such as server signing, protecting the entire domain from NTLM relay is virtually impossible. If it weren't bad enough already, we will present several new ways to abuse this infamous authentication protocol, including a new critical zero-day vulnerability we have discovered which enables to perform NTLM Relay and take over any machine in the domain, even with the strictest security configuration, while bypassing all of today's offered mitigations. Furthermore, we will present why the risks of this protocol are not limited to the boundaries of the on-premises environment and show another vulnerability which allows to bypass various AD-FS restrictions in order to take over cloud resources as well.

## PLEASE INJECT ME, A X64 CODE INJECTION

Friday at 16:00 in Track 1  
20 minutes | Demo

**Alon Weinberg**

Security Researcher, Deep Instinct

Malware authors are always looking for new ways to achieve code injection, thereby allowing them to run their code in remote processes. Code Injection allows hackers to better hide their persistence, gain persistence and leverage other processes' data and privileges.

Finding and implementing new, stable methods for code injection is becoming more and more challenging as traditional techniques are now widely detected by various security solutions or limited by native OS protections.

Inject-Me is a new method to inject code to a remote process in x64. Inject-Me is in fact "injection-less"—the remote (target) process is manipulated

# PRESENTATIONS

to read data from the injecting process, copy and execute it. The manipulation is mainly based on abusing ReadProcessMemory and calling conventions in X64. In addition to presenting Inject-Me, the talk will mention a generalized approach to copying data in remote processes to recreate shellcode from the injecting process.

## I KNOW WHAT YOU DID LAST SUMMER: 3 YEARS OF WIRELESS MONITORING AT DEF CON

Friday at 16:00 in Track 2  
20 minutes | Demo, Tool

**d4rkm4tter (Mike Spicer)**  
Hacker

For the past 3 years d4rkm4tter has been obsessed with monitoring the wireless networks at DEF CON. This talk will take you on a journey through the successes and failures that lead to the creation of the WiFiCactus and the over 1 TB of data captured. A history of each capture project including a summary of the most interesting pieces of data will be shown.

Many people spread a lot of fear, uncertainty and doubt about the wireless environments during DEF CON. This presentation aims to bring some clarity to what is really happening in the airwaves during one of the largest hacker conferences in the world. This will include presenting data on the attacks and sensitive information that exists in the airwaves. This presentation will demonstrate the risks of using wireless networks and information leaks that can be captured by anyone who is passively listening. Countermeasures and protection strategies will be provided to help you avoid having your data captured by those who might be listening.

With the number of connected devices around us, there has never been a better time to start wardriving or warwalking. Everyone is capable of profiling wireless data around them thanks to cheap hardware and open source tools. As hackers it is important for us to discover issues and vulnerabilities while validating claims of security by software and hardware vendors. Monitoring wireless communication is a great way to start validating those claims. All of the hardware and methods used will be provided so that anyone can do this type of monitoring on their own. Hack the Planet!

## SURVEILLANCE DETECTION SCOUT - YOUR LOOKOUT ON AUTOPILOT

Friday at 16:00 in Track 3  
20 minutes | Demo, Tool

**Truman Kain**  
Sr. Information Security Analyst at Tevora

Surveillance detection routes are a daily occurrence for clandestine operatives and agents all over the world. These mentally taxing counter-surveillance measures often mean the difference between life and death. Surveillance Detection Scout hopes to ease that burden. Scout currently supports Tesla Models S, 3 and X, running license plate recognition on 3

camera feeds to alert you in real time if you're being followed. When you park, Scout remains vigilant, implementing familiar face detection as well. By combining timestamped vehicle location data & video, computer vision and an intuitive web interface, it becomes apparent that Scout has just as many offensive as defensive applications. Over time, SDS captures and reports on observed patterns of life, allowing you to quickly gain an overview of your surroundings (or your target) with minimal effort. Whether you're conducting or evading surveillance, Scout has got you 6.

## THE JOP ROCKET: A SUPREMELY WICKED TOOL FOR JOP GADGET DISCOVERY, OR WHAT TO DO IF ROP IS TOO EASY

Friday at 16:00 in Track 4  
20 minutes | Demo, Tool

**Dr. Bramwell Brizendine**  
Assistant Professor of Computer and Cyber Sciences, Dakota State University

**Dr. Joshua Stroschien**  
Assistant Professor of Cyber Security/Network & Security Administration, Dakota State University

Return-oriented Programming (ROP) has been the predominate code-reuse attack for over a decade, but there are other options. Many mitigations can detect ROP due to heuristics, but these fail to detect Jump-oriented Programming (JOP). The JOP ROCKET is a reverse engineering framework dedicated to facilitating JOP exploits. It allows hackers to discover JOP gadgets. This includes dispatcher gadget's, which helps to subvert and direct the control flow, and functional gadgets, our primitives. This tool provides numerous options to give hackers flexibility on how to find gadgets, to narrow and expand possibilities. Additionally, the tool uses opcode-splitting to discover many unintended gadgets. All gadgets are classified based on operation as well as registers used and affected. Thus, hackers could easily obtain the desired functional gadgets, such as MOV EBX, [VALUE], using simple language commands. Because of JOP's much more complex set up, the tool provides this classification, so time isn't wasted hunting through results.

JOP is rarely done in the wild. Part of that complexity is in set up, but another part is the lack of dedicated tools. Having to find JOP gadgets manually could be time-consuming and require expertise. JOP ROCKET simplifies that, allowing the JOP gadgets to be found quickly and easily.

This talk will give brief content on ROP, and then it introduces JOP and its history. Then we will dive into JOP ROCKET, discussing its features, how to use it to find JOP gadgets, and how to set up your own JOP exploit. We will then demo the tool.



## POKING THE S IN SD CARDS

Friday at 16:30 in Track 1  
20 minutes | Demo, Tool, Exploit

**Nicolas Oberli**

Cybersecurity Expert, Kudelski security

Ever wonder why the S in SD cards stands for Secure? Well, it turns out that it is possible to read and/or write protect these cards by software using specific commands. As you might expect, this process isn't as "secure" as the name implies leading to multiple issues. This talk will present some of these features and the vulnerabilities discovered while poking at cards from various manufacturers. The equipment used in this talk is quite easily attainable allowing for easy replication and learning about these attacks.

## CAN YOU TRACK ME NOW? WHY THE PHONE COMPANIES ARE SUCH A PRIVACY DISASTER

Friday at 16:30 in Track 2  
20 minutes

**U.S. Senator Ron Wyden**

U.S. Senator from Oregon. Senate Finance Ranking Member

Amidst the current public outcry about privacy abuses by corporate america, one sector has received far less scrutiny than it deserves: phone companies. America's phone companies have a hideous track record on privacy. During the past two decades, these descendants of "Ma Bell" have been caught, repeatedly, selling (or giving away) their customers' sensitive data to the government, bounty hunters, private investigators, data brokers, and stalkers.

The DEF CON community is familiar with the phone companies' role in the Bush-era "warrantless wiretapping" program and the NSA's surveillance of telephone metadata, revealed by Edward Snowden. Far fewer people know that the carriers were also willing participants in a massive Drug Enforcement Administration (DEA) spying program, which the government quietly shut down after two decades in 2013.

Even less well-understood is how these corporations reap profits by selling our information to the private sector. As just one example, the carriers for years used shady middlemen to provide nearly unlimited access to Americans' location data to anyone with a credit card.

Join Oregon Senator Ron Wyden to learn why the phone companies have gotten one free pass after another, and what he's doing to hold them accountable.

## BREAKING THE BACK END! IT IS NOT ALWAYS A BUG. SOMETIMES, IT IS JUST BAD DESIGN!

Friday at 16:30 in Track 3  
20 minutes | Demo, Exploit

**Gregory Pickett**

Cybersecurity Operations, Hellfire Security

Reverse engineering is critical to exploitation. However, going through the process of reverse engineering can often lead to a great deal more than just uncovering a bug. So much so that you might find what you need for exploitation even if you don't find a bug.

That's right. If you go through object data, object representation, object states, and state changes enough you can find out quite a lot. Yes. Poor application logic is a bitch. Just ask any application penetration tester. This time it is not the magstripe. It's appsec and you will get to see how application attacks can be used against a hardware platform.

In this talk, I will go through the journey that I took in reverse engineering the public transportation system of an east asian mega-city, the questions that I asked as I wondered "How does this work?", the experiments that I ran to answers those questions, what I learned that lead me to an exploit capable of generating millions of dollars in fake tickets for that very same system, and how other designers can avoid the same fate. Not without risk, this research was done under a junta so I will also be telling you how I kept myself out of jail while doing it. Please join me. You won't want to miss it.

## RE: WHAT'S UP JOHNNY?--COVERT CONTENT ATTACKS ON EMAIL END-TO-END ENCRYPTION

Friday at 16:30 in Track 4  
20 minutes | Demo, Exploit

**Jens Müller**

Ruhr University Bochum

We show practical attacks against OpenPGP and S/MIME encryption and digital signatures in the context of email. Instead of targeting the underlying cryptographic primitives, our attacks abuse legitimate features of the MIME standard and HTML, as supported by email clients, to deceive the user regarding the actual message content. We demonstrate how the attacker can unknowingly abuse the user as a decryption oracle by replying to an unsuspecting looking email. Using this technique, the plaintext of hundreds of encrypted emails can be leaked at once. Furthermore, we show how users could be tricked into signing arbitrary text by replying to emails containing CSS conditional rules. An evaluation shows that 17 out of 19 OpenPGP-capable email clients, as well as 21 out of 22 clients supporting S/MIME, are vulnerable to at least one attack. We provide different countermeasures and discuss their advantages and disadvantages.

Jens Müller is a PhD student at the Chair for Network and Data Security, Ruhr University Bochum, Germany. His research interests are legacy protocols and data formats, for which he loves to investigate what could possibly go wrong in a

# PRESENTATIONS

modern world. He has experience as a speaker on international security conferences (BlackHat, IEEE S&P, OWASP) and as a freelancer in network penetration testing and security auditing. Besides breaking things, he develops free open source software, for example, tools related to network printer exploit^H^H^H^H^H^H, um, “debugging”.

## DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

Friday at 20:00 in Firesides Lounge  
120 minutes

**Christian “quaddi” Dameff**

Medical Director of Security at The University of California San Diego

**Jeff “r3plican” Tully MD**

Anesthesiologist at The University of California Davis

**Suzanne Schwartz MD**

Associate Director for Science and Strategic Partnerships at the US Food and Drug Administration FDA

**Marie Moe PhD**

Researcher and Hacker

**Billy Rios**

Founder of Whitescope

**Jay Radcliffe**

Security Researcher at Thermo Fisher Scientific

Technology’s promise flows within medicine like blood through veins. With every drip of life-saving medicine given to the smallest babies, with every paced beat of a broken heart, connected tech has changed the way we treat patients and offers near limitless potential to improve our health and wellness. But it’s taken an army of dedicated protectors to ensure that such promise isn’t outweighed by peril- and hackers are fighting on the front lines to safeguard medical devices and infrastructure so they remain worthy of our trust. Join docs quaddi and r3plican as they once again curate a selection of medicine’s finest hackers and allies for DO NO H4RM- the uniquely DEF CON conversation between the unsung heroes in the healthcare space- security researchers and advocates working to protect patients one broken med device at a time. Spun from an off-con hotel room gathering between friends into progressively in demand talks at DC 25 and 26, we’ve returned to bring you insight and inspiration- divorced from the spin and formality of an increasingly industry-saturated landscape- from the people whose primary goal is to kick ass and save lives.

## PANEL: DEF CON GROUPS

Friday at 22:15 in Firesides Lounge  
45 minutes

**Brent White / BITK1LL3R**

Global Coordinator

**Jayson E. Street**

Ambassador

**Darington**

Web Master

**April Wright**

Welcoming Committee & Liaison

**Tim Roberts (byt3boy)**

Volunteer

**Casey Bourbonnais**

Volunteer

**sOups**

Social media

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 fireside chat, your DEF CON groups team who works behind the scenes to make DCG possible will invite group leaders to share how they started their groups, how they found meeting space, how they decide what content to present each meeting, and other topics. Potential new group leaders can find out how to start and run a local group, and existing group leaders and members can share and get operational ideas for running the best group possible. During the Fireside chat, we’ll have the ability to keep it an open forum for questions and ideas, as well as a great opportunity to meet other groups.

## SATURDAY

### WEAPONIZING HYPERVISORS TO FIGHT AND BEAT CAR AND MEDICAL DEVICES ATTACKS

Saturday at 10:00 in Track 1  
45 minutes | Demo, Tool

**Ali Islam**

CEO, Numen Inc.

**Dan Regalado (DanuX)**

CTO, Numen Inc

Historically, hypervisors have existed in the cloud for efficient utilization of resources, space, and money.

The isolation feature is one of the reasons hypervisors are heavily moving to other ecosystems, like Automobiles, so that for example, if an Infotainment crashes, it does not affect other sensitive ECUs like ADAS. Blackberry QNX and AGL announced the use of hypervisors in their deployments on Cars.

The trending is real, but there is a big challenge!



# FRIDAY/SATURDAY

Most of the systems in Cars and Medical devices run on ARM, plus, protection at the hypervisor level is still limited. So, is it possible to have a framework that runs at the hypervisor level, able to monitor at the OS level and most important, capable to identify and kill threats coming into the monitored devices?

During this talk we will walk you through the steps needed to setup a framework running on Xilinx ZCU102 board able to monitor ARM-based devices and to kill malicious threats identified. Also will discuss challenges on syscall monitoring, single-stepping limitations, techniques to stay stealthy, techniques to detect and kill traditional malware seen in enterprise like Ransomware, Heap Exploits and capabilities on VM Escape attacks and feasibility to detect Spectre-like exploits.

## RISE OF THE HYPEBOTS: SCRIPTING STREETWEAR

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

**finalphoenix**  
Engineer & Hypebae

Buying Supreme is even harder when most of your competitors are AI. The era of bot purchasing has arrived and more often than not, purchasing shoes, shirts, and swag, requires shell scripting. We will look at how simplistic (and how complicated) purchasing bots have become, how to write them, and what companies are trying to do to fight them, and why they're failing at conquering the machines.

## INFORMATION SECURITY IN THE PUBLIC INTEREST

Saturday at 10:00 in Track 3  
45 minutes

**Bruce Schneier**

Computer security is now a public policy issue. Election security, blockchain, "going dark," the vulnerabilities equities debate, IoT safety, data privacy, algorithmic security and fairness, critical infrastructure: these are all important public policy issues with a strong Internet security component. But while an understanding of the technology involved is fundamental to crafting good policy, there is little involvement of technologists in policy discussions. This is not sustainable. We need public-interest technologists: people from our fields helping craft policy, and working to provide security to agencies and groups working in the broader public interest. We need these people in government, at NGOs, teaching at universities, as part of the press, and inside private companies. This is increasingly critical to both public safety and overall social welfare. This talk both describes the current state of public-interest technology, and offers a way forward for us individually and collectively for our field. The defining policy question of the Internet age is this: How much of our lives should be governed by technology, and under what terms? We need to be involved in that debate.

## EDR IS COMING; HIDE YO SHIT

Saturday at 10:00 in Track 4  
45 minutes | Demo, Tool

**Michael Leibowitz**  
Principal Troublemaker

**Topher Timzen**  
(@TTimzen), Principal Vulnerability Enthusiast

There's a new, largely unaddressed threat in the security industry today, Endpoint Detection and Response (EDR), which aims to stop threat actors in their tracks. The scenario plays out like this... At first your campaign is going well and your attacker objectives are being met. Then, your lovingly crafted payloads become analyst samples, you're evicted from the environment and you lose your persistence. You and the analyst are now having a bad time. You may feel this is just fear mongering, but we assure you, the risk is real. Fortunately, we have a few new tricks up our sleeves to keep this nightmare scenario at bay. While many would have you believe that we live in a measured and signed boot Utopia on modern systems, we will show you the seedy underbelly of this Brave New World. By abusing early boot mechanisms and UEFI platform firmware, we are able to evade common detection. By showing up early to the fight, we sucker punch EDR, leaving it in a daze unable to see our malicious activities. We put a new twist on old code injection techniques and maintain persistence in UEFI firmware, making an effective invisibility cloak. By leveraging these two techniques, you and the analyst can have a happy and relaxing evening. From that point on - the good ol' days are back again! Plunder away!

## YOUR CAR IS MY CAR

Saturday at 11:00 in Track 1  
45 minutes | Demo, Tool, Exploit

**Jmaxxx**

For many of us, our cars are one of the largest purchases we will ever make. In an always connected world it is natural that we would want to have the convenience of being able to remotely monitor our vehicles: to do everything from remind ourselves exactly where exactly we parked, verify we locked our vehicle, or even remote start it so it will be warmed up (or cooled down) when we get in. There are a variety of vendors offering aftermarket alarm systems that provide these conveniences and offer a peace of mind. But how much can we trust the vendors of these systems are protecting access to our cars in the digital domain? In this talk, Jmaxxx will tell the story of what he found when he looked into one such system.

## HAKC THE POLICE

Saturday at 11:00 in Track 2  
45 minutes | Demo, Tool

**Bill Swearingen**  
World's #23 Best Hacker

PULL OVER!

# PRESENTATIONS

No, it is a cardigan, but thanks for noticing!

After getting a nasty speeding ticket, OG SecKC HA/KC/ER hevnsnt decided enough was enough, and set out to fully understand police speed measurement devices, and develop homebrew countermeasures that are legal in some states (and some that are not). Come learn how police RF (X, K, KA) and Laser speed detection systems work and how to implement your own homebrew jamming countermeasures on the cheap, essentially making your vehicle invisible to law enforcement. HOP IN and BUCKLE UP, this talk is going to FUEL your hardware hacking desires! You better be able to think fast to keep up with this talk and prepare to get home in record time.

## HACKING YOUR THOUGHTS - BATMAN FOREVER MEETS BLACK MIRROR

Saturday at 11:00 in Track 3

45 minutes

**Katherine Pratt/GattaKat**

NSF Graduate Research Fellow, University of Washington - Seattle

Companies are coming for your brains. The electricity in your brains, to be more precise. Valve, Facebook, Elon Musk and more are funding research into technologies that will translate neural signals into controls for devices like computers, smartphones, and VR/AR environments. While this would be super exciting, it represents some serious data privacy issues. First: what kind of private information can be elicited from your neural signals? It's possible to use a specific kind of neural response to visual and audio stimuli to deduce information about the user... like where you bank, who you know, your real identity, etc (Edward Nygma in Batman Forever, anyone?)

More broadly, there is also the issue of what happens when you provide your neural signals to a company. If you're worried about what Facebook is doing with your information now, imagine what they can do when they have hours of information straight from your brain. If neural data is treated the same as your DNA, commercial companies become the owners of your thoughts (as electrical signals). Will they readily share it with the FBI without probable cause? These kinds of questions, and many more, are starting to surface with neurally-controlled devices and other emerging technologies. This talk will cover all of this and more.

## METICULOUSLY MODERN MOBILE MANIPULATIONS

Saturday at 11:00 in Track 4

45 minutes | Demo

**Leon Jacobs**

Researcher - SensePost

Mobile app hacking peaked in 2015 with tools like keychain-dumper & ssl-kill-switch released but requiring jailbroken/rooted devices. Back then, wrestling the power to understand & modify apps on our devices from dystopian looking mega corps was our cause. As jailbreaks became infrequent, the

hackers' arsenal was left behind. While this is progress against dark uses of hacking, done to protect our freedom fighters, how can hackers still hold power to account? Can we still find flaws in apps/devices & live up to the protections the technology promises?

Enter runtime binary instrumentation with Frida. It's possible to analyze apps in their final state when executed on real hardware running the latest iOS/Android with no jailbreaks. This fills a gap between source analysis & debuggers. But, simply enumerating app classes requires studying multiple blogs & a deep read of the docs. We created Objection to simplify this & hide the boilerplate so hackers could focus on unravelling apps. But, many people still rely on simple hacks & automation & rarely use new advanced techniques such as reflectively inspecting live heap objects, canary execution tracing, runtime memory edits and filesystem exploration.

We'll show hackers, malware researchers & security engineers how to use these advanced mobile hacking techniques.

## HOW YOU CAN BUY AT&T, T-MOBILE, AND SPRINT REAL-TIME LOCATION DATA ON THE BLACK MARKET

Saturday at 12:00 in Track 1

45 minutes

**Joseph Cox**

Senior Staff Writer, Motherboard

Major US telecommunications companies AT&T, T-Mobile, and Sprint have been quietly selling access to their customers' real-time location data, including cell tower information as well as highly precise GPS data. Through a complex network of dodgy data aggregators and middlemen companies, this data access eventually trickled down to a slew of different industries, used car salesman, landlords, and hundreds of bounty hunters, likely without your knowledge or informed consent. In this talk, based on leaked documents, sources, and first hand experience, Joseph will explain how this data industry works, the players involved, and also how the data access is available on the black market, where it can be used in any way an attacker fancies: Joseph paid a source \$300 to successfully locate a phone in New York.

## DEFEATING BLUETOOTH LOW ENERGY 5 PRNG FOR FUN AND JAMMING

Saturday at 12:00 in Track 2

45 minutes | Demo, Tool

**Damien Cauquil (virtualabs)**

Senior Security Researcher @ Econocom Digital.Security

Bluetooth Low energy version 5 has been published in late 2016, but we still have no sniffer supporting this specific version (and not that much compatible devices as well). The problem is this new version introduces a new channel hopping algorithm that renders previous sniffing tools useless as devices can no longer be



attacked and connections analyzed. This new algorithm is based on a brand new pseudo-random number generator (PRNG) to provide better collision avoidance while kicking out all of our good old sniffing tools.

Unless some random hacker manages to break this not-that-strong PRNG and upgrades his BLE sniffing tool to support this algorithm ;). In this talk, we will explain why this PRNG is vulnerable and how it can be easily defeated to sniff and jam communications between two BLE 5 devices. A new version of BtleJack will be released during this talk, providing an efficient way to sniff BLE 5 connections to our fellow IoT hacker family.

## WHY YOU SHOULD FEAR YOUR “MUNDANE” OFFICE EQUIPMENT

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

**Daniel Romero**

Managing Security Consultant, NCC Group

**Mario Rivas**

Senior Security Consultant, NCC Group

The security of common enterprise infrastructure devices such as desktops and laptops has advanced over the years through incremental improvements in operating system and endpoint security. However, security controls for network devices such as enterprise printers are often ignored and thus present a greater potential for exploitation and compromise by threat actors seeking to gain a persistent foothold on target organisations.

In order to assess the current state of mainstream enterprise printer product security and to challenge common assumptions made about the security of these devices, which sit on key parts of enterprise networks and process sensitive data, we set out on a vulnerability and exploitation research project of six known vendors. We were able to find remote vulnerabilities in all printers tested through various attack vectors, revealing a large number of 0-day vulnerabilities in the process.

In this talk we walk through the entire research engagement, from initial phases such as threat modelling to understand printer attack surfaces to the development of attack methodologies and fuzzing tools used to target printer-specific protocols and functions. Besides of remarking important vulnerabilities found and their respective CVE's, proof of concept exploits showing how it is possible to gain full control of printers and all of the data they manage will be presented. This will show how to use enterprise printers as a method of persistence on a network, perhaps to exfiltrate sensitive data or support C2 persistence on Red Team engagements.

We also address a number of challenges that researchers can face when performing vulnerability research on devices such as printers and how we used different techniques to overcome these challenges, working with limited to no debugging and triage capabilities. We also present mitigations that printer manufacturers can implement in order to reduce printer attack surfaces and render exploitation more difficult.

## ZOMBIE ANT FARM: PRACTICAL TIPS FOR PLAYING HIDE AND SEEK WITH LINUX EDRs

Saturday at 12:00 in Track 4  
45 minutes | Demo, Tool

**Dimitry Snezhkov**

Sr. Security Consultant, X-Force Red

EDR solutions have landed in Linux. With the ever increasing footprint of Linux machines deployed in data centers, offensive operators have to answer the call.

In the first part of the talk we will share practical tips and techniques hackers can use to slide under the EDR radar, and expand post-exploitation capabilities.

We will see how approved executables could be used as decoys to execute foreign functionality. We will walk through the process of using well known capabilities of the dynamic loader. We will take lessons from user-land root-kits in evasion choices.

Part two will focus on weaponizing the capabilities. We will show how to create custom preloaders, and use mimicry to hide modular malware in memory. We will create a “Preloader-as-a-Service” capability of sorts by abstracting storage of modular malware from its executing cradles. This PaaS is free to you though!

We fully believe the ability to retool in the field matters, so we have packaged the techniques into reusable code patterns in a toolkit you will be able to use (or base your own code on) after it is released.

This talk is for hackers, offensive operators, malware analysts and system defenders. We sincerely hope defensive hackers can attend and also have fun.

## RACE - MINIMAL RIGHTS AND ACE FOR ACTIVE DIRECTORY DOMINANCE

Saturday at 13:00 in Track 1  
45 minutes | Demo, Tool

**Nikhil Mittal**

PentesterAcademy

User rights and privileges are a part of the access control model in Active Directory. Applicable only at the local computer level, a user generally has different rights (through access tokens) on different machines in a domain. Another part of the access control model is security descriptors (ACLs) that protects a securable object. At the domain level, ACL abuse is well known and adversaries have used it for persistence. For user rights, the abuse is mostly with the help of groups (memberships, SID History etc.) or misconfigured delegated rights.

A lesser-known area of abuse and offensive research is a combination of minimal Rights and ACE (hence the term RACE). Often overlooked in audits and assessments, using minimal rights along with favourable ACEs provides a very interesting technique of persistence and on-demand privilege escalation on a Windows machine with much desired stealth.

This talk covers interesting domain privilege escalation, persistence and backdoor techniques with the help

# PRESENTATIONS

of ACLs, minimal user rights and combinations of both. We will discuss how these techniques can be applied using open source tools and scripts. The talk also covers how to detect and mitigate such attacks.

The talk will be full of live demonstrations.

## GSM: WE CAN HEAR EVERYONE NOW!

Saturday at 13:00 in Track 2

45 minutes | Demo, Exploit

**Campbell Murray**

Global Head Cybersecurity Delivery, BlackBerry

**Eoin Buckley**

Senior Cybersecurity Consultant

**James Kulikowski**

Senior Cybersecurity Consultant

The presentation demonstrates that the security of the A5/1 and A5/3 ciphers used to protect cellular calls are vulnerable to compromise leading to full decryption of GSM communications, using freely available open source solutions along with our tools we developed for this task.

The flaw being exploited lies in the heart of the design of GSM. In all implementations the standard requires GSM messages to first be error control encoded using a convolutional code and then encrypted. In the vast majority of implementations used today, encryption is performed using the A5/1 or A5/3 cipher. The convolutional code adds redundancy to the transmitted message, which can act like a fingerprint to identify the key used to encrypt the GSM message.

To exploit the vulnerability an attacker simply needs to capture a transmission and identify the GSM channel used. The standard defines the convolutional code and therefore how the redundancy may be interpreted to recover the encryption key.

This presentation considers passively capturing GSM traffic using A5/3 encryption and demonstrates a novel solution to cracking the key used without interacting with the mobile or network.

## TAG-SIDE ATTACKS AGAINST NFC

Saturday at 13:00 in Track 3

45 minutes | Demo, Tool

**Christopher Wade**

This talk covers tag-side attacks against NFC communication protocols, including cracking of Mifare encryption keys and performing targeted attacks against NFC readers. In addition, it will cover the design and creation of devices capable of emulating NFC tags down to the raw protocol using standard components and tools, with no abstraction to dedicated hardware, covering and expanding on the capabilities of available products. This talk will contain how 13.56MHz NFC works at a raw level, how tools can be built for analysing it, how the protocol can be implemented in full on standard Microcontrollers, and the security weaknesses present in its design.

## SSO WARS: THE TOKEN MENACE

Saturday at 13:00 in Track 4

45 minutes | Demo, Tool, Exploit

**Alvaro Muñoz**

Software Security Researcher @ Fortify (Micro Focus)

**Oleksandr Mirosh**

Software Security Researcher @ Fortify (Micro Focus)

It is the year 2019. Humanity has almost won its long-standing war against Single-Sign On (SSO) bugs. The last of them were discovered and eradicated some time ago and the world is now living in an era of prosperity while the Auth Federation enjoys peaceful CVE-free times. However, while things seem to be running smoothly, new bugs are brewing at the core of major implementation libraries. This is probably the last chance for the evil empire to launch a world scale attack against the Auth Federation.

In this talk, we will present two new techniques:

1) A new breed of SAML implementation flaws that break XML signature validation and enable arbitrary modification of the SAML assertion, which enables attackers to authenticate as arbitrary users or grant themselves arbitrary authorization claims. Although any implementation may be affected by this flaw, we will show how it affects Microsoft Windows Identity Framework (WIF) applications, Windows Communication Foundation (WCF) web services, and flagship products such as SharePoint and Exchange Servers.

2) A bug in the .NET crypto library, which may allow attackers to gain Remote Code Execution (RCE) or Denial of Service (DoS) depending on the availability of code gadgets in the target server.

A new tool to detect this type of vulnerability will also be discussed and released.

## SELECT CODE \_ EXECUTION FROM \* USING SQLITE;—GAINING CODE EXECUTION USING A MALICIOUS SQLITE DATABASE

Saturday at 14:00 in Track 1

45 minutes | Demo, Tool, Exploit

**Omer Gull**

Security Researcher at Check Point Software Technologies

Everyone knows that databases are the crown jewels from a hacker's point of view, but what if you could use a database as the hacking tool itself? We discovered that simply querying a malicious SQLite database - can lead to Remote Code Execution. We used undocumented SQLite3 behavior and memory corruption vulnerabilities to take advantage of the assumption that querying a database is safe.

How? We created a rogue SQLite database that exploits the software used to open it. Exploring only a few of the possibilities this presents we'll pwn password stealer backends while they parse credentials files and achieve iOS persistence by replacing its Contacts database...



The landscape is endless (Hint: Did someone say Windows 10 0-day?). This is extremely terrifying since SQLite3 is now practically built-in to any modern system.

In our talk we also discuss the SQLite internals and our novel approach for abusing them. We had to invent our own ROP chain technique using nothing but SQL CREATE statements. We used JOIN statements for Heap Spray and SELECT subqueries for x64 pointer unpacking and arithmetics. It's a new world of using the familiar Structured Query Language for exploitation primitives, laying the foundations for a generic leverage of memory corruption issues in database engines.

## I'M ON YOUR PHONE, LISTENING - ATTACKING VOIP CONFIGURATION INTERFACES

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

**Stephan Huber**

Fraunhofer SIT

**Philipp Roskosch**

If toasters talking to fridges is no joke to you, then you are aware of the big Internet of Things hype these days. While all kind of devices get connected and hacked, one of the oldest class of IoT devices seems to be forgotten even though it is literally everywhere - VoIP phones.

For configuration and management purposes, VoIP phones run a web application locally on the device. We found several critical bugs (reported CVEs) in the web application as well as in the webserver which enabled us to hijack the phones. Starting with simple XSS and CSRF issues, via command injections and memory corruptions right through to remote code executions, all popular vulnerability classes can be found on those devices.

We will present our findings together with the tools and strategies we used, and will enable you to do the same with your own phones and other IoT devices.

Further, we will provide helpful ARM shell code patterns, scripts and tricks which hackers can use to find bugs. We will conclude our talk by showing that automatic tools fail to discover such vulnerabilities. Therefore, manual IoT pentesting is still required.

If you think these management interfaces are not exposed to the internet, you are wrong. In a scan, we found thousands of reachable phones vulnerable to our exploits.

## ZERO BUGS FOUND? HOLD MY BEER AFL! HOW TO IMPROVE COVERAGE-GUIDED FUZZING AND FIND NEW ODAYS IN TOUGH TARGETS

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

**Maksim Shudrak**

Security Researcher

Fuzzing remains to be the most effective technique for bugs hunting in memory-unsafe programs. Last year, hundreds of security papers and talks on fuzzing have been published and dozens of them were focused on adapting or improving American Fuzzy Lop in some way. Attracting with its simplicity and efficiency, AFL is the number one choice for the vast majority of security researchers. This high popularity means that hunting for bugs with AFL or a similar tool is becoming less and less fruitful since many projects are already covered by other researchers. It is especially hard when we talk about a project participating in Google OSS-Fuzz program which utilizes AFL to generate a half-trillion test cases per day.

In practice, this means that we can not blindly rely on AFL anymore and should search for better fuzzing techniques. In order to overcome this challenge, we need to understand how AFL and similar fuzzers work and be able to use their weaknesses to find new 0days. This talk is aimed to discuss these weaknesses on real examples, explain how we can do fuzzing better and release a new open-source fuzzer called Manul.

Manul is a high-scalable coverage-guided parallel fuzzer with the ability to search for bugs in open source and black box binaries on Windows and Linux. Manul was able to find 10 0-days in 4 widely-used projects that have been extensively tested by AFL. These vulnerabilities were not found by chance, but by analyzing and addressing issues exist in AFL. Authors will show several of the most critical vulnerabilities and explain why AFL overlooked them.

This talk will be interested for experienced hackers, who are willing to improve their bug hunting capabilities, as well as for new researchers, who are making their first steps on the thorny trail of bug hunting.

## NEXT GENERATION PROCESS EMULATION WITH BINEE

Saturday at 14:00 in Track 4  
45 minutes | Demo, Tool

**Kyle Gwinnup**

Senior Threat Researcher, Carbon Black

**John Holowczak**

Threat Researcher

The capability to emulate x86 and other architectures has been around for some time. Malware analysts have several tools readily available in the public domain. However, most of the tools stop short of full emulation, halting or doing strange things when emulating library functions or system calls not implemented in the emulator. In this talk we introduce

# PRESENTATIONS

a new tool into the public domain, Binee, a Windows Process emulator. Binee creates a nearly identical Windows process memory model inside the emulator, including all dynamically loaded libraries and other Windows process structures. Binee mimics much of the OS kernel and outputs a detailed description of all function calls with human readable parameters through the duration of the process. We've designed Binee with two primary use cases in mind; data extraction at scale with a cost and speed similar to common static analysis tools, and second, for malware analysts that need a custom operating system and framework without the overhead of spinning up various configurations of virtual machines. Currently Binee can run on Windows, OS X, and Linux.

## GET OFF THE KERNEL IF YOU CAN'T DRIVE

Saturday at 15:00 in Track 1  
45 minutes | Demo, Tool, Exploit

**Jesse Michael**

Mickey Shkatov

For software to communicate with hardware, it needs to talk to a kernel-mode driver that serves as a middleman between the two, helping to make sure everything operates as it should. In Windows that is done using the Kernel-Mode Driver Framework (KMDF).

These drivers are used to control everything in your computer, from small things like CPU fan speed, color of your motherboard LED lights, up to flashing a new BIOS.

However, as the code in these drivers runs with the same privileges as the rest of the kernel, malicious drivers can be used to compromise the security of the platform. To that end, Microsoft relies on WHQL, code signing, and EV Signing to prevent drivers which have not been approved by Microsoft from being loaded into the kernel.

Unfortunately, security vulnerabilities in signed drivers can be used to as a proxy to read and write hardware resources such as kernel memory, internal CPU configuration registers, PCI devices, and more. These helpful driver capabilities can even be misused to bypass and disable Windows protection mechanisms.

Let us teach you how these drivers work, show you the unbelievable risk they pose, and enjoy our walk of shame as we parade all the silly and irresponsible things we discovered in our research.

## REVERSE-ENGINEERING 4G HOTSPOTS FOR FUN, BUGS AND NET FINANCIAL LOSS

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

**g richter**

Senior Researcher, Pen Test Partners LLP

"5G is coming" (apparently). That probably means, over the next few years, more and more people are going to be using more and more cellular-connected devices for their day-to-day TCP/IP activities.

The problem is, a lot of existing 4G modems and routers are pretty insecure. We found critical remotely-exploitable flaws in a selection of devices from variety of vendors, without having to do too much work. Plus, there's only a small pool of OEMs working seriously with cellular technologies, and their hardware (& software dependencies) can be found running in all sorts of places. Their old 4G, 3G and even 2G-era code is going to be running in these 5G-capable devices.

With a small sample of consumer 4G routers as examples, we're going to talk about how malleable, frustrating, and insecure these devices are. We'll run through a few examples of existing 4G routers, from low-end bargain-basement end-of-life-never-to-be-fixed to higher-end devices. root is a means to an end, rather than the goal.

## STATE OF DNS REBINDING - ATTACK & PREVENTION TECHNIQUES AND THE SINGULARITY OF ORIGIN

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

**Gerald Doussot**

Principal Security Consultant, NCC Group

**Roger Meyer**

Principal Security Consultant, NCC Group

Do you want to know how you can exploit DNS rebinding 10x faster, bypass prevention mechanisms, interactively browse the victim's internal network, and automate the whole process during your next red team exercise?

This talk will teach you how and give you an easy-to-use tool to do it.

First, we will cover in detail the subtleties that make DNS rebinding attacks more effective in practice, including techniques and operational conditions that make it faster and more reliable. We'll also explain how to bypass commonly recommended security controls, dispelling attack and defense misconceptions that have been disseminated in blogs and social media posts.

This talk will include a number of demos using Singularity, our open source DNS rebinding attack framework that includes all the parts you need to get started pwning today, including:

- Remote code execution and exfiltration payloads for common dev tools and software
- Practical scanning and automation techniques to maximize the chance of controlling targeted services

We'll also show an interesting post-exploitation technique that allows you to browse a victim browser network environment via the attacker's browser without the use of HTTP proxies.

You'll leave this talk with the knowledge and tools to immediately start finding and exploiting DNS rebinding bugs.



# SATURDAY

## .NET MALWARE THREATS: INTERNALS AND REVERSING

Saturday at 15:00 in Track 4  
45 minutes

**Alexandre Borges**

Security Researcher at Blackstorm Security

.NET malware is well-known by security analysts, but even existing many tools such as dnSpy, .NET Reflector, de4dot and so on to make the analysis easier, most professionals have used them as a black box tool, without concerning to .NET internals, structures, MSIL coding and details. In critical cases, it is necessary have enough knowledge about internal mechanisms and to debug these .NET threats using WinDbg.

Unfortunately, .NET malware samples have become very challenger because it is so complicated to deobfuscated associated resources, as unpacking and dumping them from memory. Furthermore, most GUI debugging tools does an inside view of mechanisms such as CRL Loader, Managed Heap, Synchronization issues and Garbage Collection.

In the other side, .NET malware threats are incredibly interesting when analyzed from the MSIL instruction code, which allows to see code injections using .MSIL and attempts to compromise .NET Runtime keep being a real concern.

The purpose of this presentation is to help professionals to understand .NET malware threats and techniques by explaining concepts about .NET internals, mechanisms and few reversing techniques.

## REVERSE ENGINEERING 17+ CARS IN LESS THAN 10 MINUTES

Saturday at 16:00 in Track 1  
20 minutes | Demo, Tool

**Brent Stone**

Brent provides a live demonstration reversing engineering 17 or more unknown passenger vehicle CAN networks in under 10 minutes using new automated techniques. These unsupervised techniques are over 90% accurate and consistent when tested using production CAN networks and different driving conditions. He then introduces the Python and R code used for the demo and posted to his public GitHub repository at [https://github.com/brent-stone/CAN\\_Reverse\\_Engineering](https://github.com/brent-stone/CAN_Reverse_Engineering). The Dissertation explaining how the code works is also posted.

## NOC NOC. WHO'S THERE? ALL. ALL WHO? ALL THE THINGS YOU WANTED TO KNOW ABOUT THE DEF CON NOC AND WE WON'T TELL YOU ABOUT

Saturday at 16:00 in Track 2  
105 minutes

### The DEF CON NOC

It's been a while, something like DEF CON 19, since we had the chance to have more than a few minutes at closing ceremonies to talk to everyone about the DEF CON NOC. It is not uncommon for people during the show or throughout the year to come to us asking things here and there about the DEF CON network. Come see all the DEF CON NOC team on stage, yes, those you usually don't see anywhere during the show, because, well, we're making sure packets are flowing and people are interning. Come learn what we do, how we do it and possibly answer any questions that you might have about the "most hostile network in the planet".

## CONFESSIONS OF AN NESPRESSO MONEY MULE: FREE STUFF & TRIANGULATION FRAUD

Saturday at 16:00 in Track 3  
20 minutes

**Nina Kollars**

Associate Professor Naval War College Strategic and Operational Research Department

**Kitty Hegemon**

In 2018 I somewhat innocently bought very expensive coffee (Nespresso capsules) online from Ebay. What followed was a series of unexpected additional packages from the manufacturer Nespresso and a lurking suspicion that something had gone terribly—if not criminally—wrong as a result of my purchase. This talk chronicles the obnoxious amounts of obsessive research and tracking that became my new hobby—stalking Nespresso fraudsters and my decidedly non-technical attempts at developing a generic search profile and reporting the fraudsters to anyone who would listen, to include : the persons whose identities had been stolen, Nespresso, Ebay, and the FBI. Ultimately I just ended up with a LOT of coffee; a lingering sense that I had committed several crimes; and no faith left in humanity.

## VACUUM CLEANING SECURITY—PINKY AND THE BRAIN EDITION

Saturday at 16:00 in Track 4  
20 minutes | Exploit

**jiska**

TU Darmstadt, Secure Mobile Networking Lab

**clou (Fabian Ullrich)**

Data collected by vacuum cleaning robot sensors is highly privacy-sensitive, as it includes details and metadata about consumers' habits, how they

# PRESENTATIONS

live, when they work or invite friends, and more. Connected vacuum robots are not as low-budget as other IoT devices and vendors indeed invest into their security. This makes vacuum cleaning robot ecosystems interesting for further analysis to understand their security mechanisms and derive takeaways.

In this talk we discuss the security of the well-protected Neato and Vorwerk ecosystems. Their robots run the proprietary QNX operating system, are locally protected with secure boot, and use various mechanisms that ensure authentication and encryption in the cloud communication. Nonetheless, we were able to bypass substantial security components and even gain unauthenticated privileged remote execution on arbitrary robots. We present how we dissected ecosystem components including a selection of vacuum robot firmwares and their cloud interactions.

## UNPACKING PKGS: A LOOK INSIDE MACOS INSTALLER PACKAGES AND COMMON SECURITY FLAWS

Saturday at 16:30 in Track 1  
20 minutes | Demo

**Andy Grant**

Technical Vice President, NCC Group

We are hackers, we won't do as you expect or play by your rules, and we certainly don't trust you. JAR files are really ZIPs...unzip them! So are Microsoft's DOCX, XLSX, PPTX, etc. Let's open them up! macOS applications (.app "files") are really directories you can browse?! Sweet, let's do that.

Less well known but similarly prevalent are Flat Package Mac OS X Installer (.pkg) files. These are actually XAR archives that, among other things, contain many plaintext files (including shell, Perl, and Python scripts) as cpio files compressed using gzip.

In this presentation I'll walk you through extracting the contents of these installer packages, understanding their structure, and seeing how they work while highlighting where security issues can come up. To drive the point home of what can go wrong, I'll include examples of serious security issues I've seen in the wild and show you how they can be exploited to elevate privileges and gain code/command execution.

After this talk, .pkg files will no longer be opaque blobs to you. You'll walk away knowing tools and techniques to tear them open, understand how to evaluate what they're really doing on your computer, and a methodology for finding bugs in them. As a final bonus, I'll include a subtle trick or two that can be used on red teams.

## GO NULL YOURSELF OR: HOW I LEARNED TO START WORRYING WHILE GETTING FINED FOR OTHER'S AUTO INFRACTIONS

Saturday at 16:30 in Track 3  
20 minutes

**droogie**

Security Consultant at IOActive

Input sanitization issues will always exist, although it's surprising at how we're still seeing amateur mistakes being made on everyday applications and systems used by millions. After making some observations against automatic license plate recognition (ALPR) data requested via the freedom of information act (FOIA) while having reminiscent conversations about old hacker tales, it turned on the evil bit, leading to some interesting ideas. We'll go over this adventure of poking at systems using totally valid user-controlled data that causes unexpected behavior in the real world. It's always a strange thing when you can "exploit" unexpected attack surface, due to poor specification, especially in government systems.

## APACHE SOLR INJECTION

Saturday at 16:30 in Track 4  
20 minutes | Demo, Exploit

**Michael Stepankin**

Security Researcher at Veracode

Apache Solr is a search platform used by many enterprise companies to add a full text search functionality to their websites. Often hidden behind firewalls, it provides a rich API to search across large datasets. If this API is used by web applications in a wrong way, it may open a possibility for injection attacks to completely modify the query logic.

In this talk we'll shed some light on the new type of vulnerabilities for web applications - Solr parameter injection, and provide some useful ways how to achieve remote code execution through it. We also provide exploits for almost all known vulnerabilities for Apache Solr, including the two new RCEs we reported this year.



# SATURDAY/SUNDAY

## MEET THE EFF - MEETUP PANEL

Saturday at 20:00 in Firesides Lounge  
120 minutes

**Kurt Opsahl**

Deputy Executive Director And General Counsel

**Camille Fischer**

Frank Stanton Fellow

**Bennett Cyphers**

Staff Technologist

**Nathan 'nash' Sheard**

Grassroots Advocacy Organizer

**Shahid Buttar**

Panel Host, Director of Grassroots Advocacy

Join staffers at the Electronic Frontier Foundation, the nation's premier digital civil liberties group fighting for freedom and privacy in the computer age, for a candid chat about how the law is racing to catch up with technological change.

Then meet representatives from Electronic Frontier Alliance allied community and campus organizations from across the country. These technologists and advocates are working within their communities to educate and empower their neighbors in the fight for data privacy and digital rights.

This discussion will include updates on current EFF issues such as the government's effort to 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, surveillance and technology issues that are important to you.

## WE HACKED TWITTER... AND THE WORLD LOST THEIR SH\*T OVER IT!

Saturday at 22:15 in Firesides Lounge  
45 minutes

**Mike Godfrey**

Penetration Tester, INSINIA Security

**Matthew Carr**

Penetration Tester, INSINIA Security

In December 2018 INSINIA Security was involved in one of the biggest hacking stories of the year. A number of "celebrities", including Louis Theroux, Eamon Holmes and more, logged into their Twitter accounts just after Christmas to find a Tweet, from their account, saying:

"This account has been temporarily hijacked by INSINIA SECURITY".

The tweet immediately directed people to our blog post, and the compromised accounts retweeted INSINIA's Tweet, saying:

"This account is now under the control of @InsiniaSRT.

Luckily, this has been H4CK3D to highlight an important vulnerability. The user of this account has NOT lost access to it, no data compromised and is NOT under attack. See how it was done..."

What we did was simple. We used spoof texts to Tweet from these accounts. We NEVER had access to these accounts. We could never read DM's. We simply passively controlled these accounts with no opportunity of getting confidential data in return.

So what did the hacking community, journalists and commentators do?! They LOST THEIR SH\*T OVER IT!

"It's unethical" "It's a crime" "Computer Misuse Act counts for security researchers too!" "You guys are total f\*cking idiots!"

These are the types of things we'd heard from our peers. But why was the backlash so bad? In this talk, INSINIA explains why it was done, how it was done, how people reacted and how research can be released quickly and responsibly... Without always getting the warm reception you might expect!

## SUNDAY

## BACKDOORING HARDWARE DEVICES BY INJECTING MALICIOUS PAYLOADS ON MICROCONTROLLERS

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

**Sheila Ayelen Berta**

Security Researcher

Is targeting microcontrollers worth the effort? Nowadays, they are responsible for controlling a wide range of interesting systems, e.g., physical security systems, car's ECUs, semaphores, elevators, sensors, critical components of industrial systems, some home appliances and even robots.

In this talk, it will be explained how microcontrollers can be backdoored too. After a quick review of basic knowledge about uC, we will dive into three different approaches to achieve payload injection, from basic to advanced techniques. The first method consists on locating the entry point of the firmware and inject our payload there, this is an easy way to execute it at least once. As a second -and more complex- technique, we will backdoor the EUSART communication injecting a malicious payload at the code routine of that hardware peripheral; we will be able to get the right memory address by inspecting the GIE, PEIE and polling process at the uC interrupt vector. Finally, the third technique allow us to take control of the microcontroller's program flow by manipulating the stack writing memory addresses at the TOS; with this we can execute a payload made with instructions already written in the original program, performing it just like a ROP-chain technique.

# PRESENTATIONS

## ADVENTURES IN SMART BUTTPLUG PENETRATION (TESTING)

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

**smea**

Analysts believe there are currently on the order of 10 billions Internet of Things (IoT) devices out in the wild. Sometimes, these devices find their way up people's butts: as it turns out, cheap and low-power radio-connected chips aren't just great for home automation - they're also changing the way we interact with sex toys. In this talk, we'll dive into the world of teledildonics and see how connected buttplugs' security holds up against a vaguely motivated attacker, finding and exploiting vulnerabilities at every level of the stack, ultimately allowing us to compromise these toys and the devices they connect to.

## HACKING WEBASSEMBLY GAMES WITH BINARY INSTRUMENTATION

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

**Jack Baker**

WebAssembly is the newest way to play video games in your web browser. Both Unity3d and Unreal Engine now support WebAssembly, meaning the amount of WebAssembly games available is growing rapidly. Unfortunately the WebAssembly specification is missing some features game hackers might otherwise rely on. In this talk I will demonstrate adapting a number of game hacking techniques to WebAssembly while dealing with the limitations of the specification.

For reverse engineers, I will show how to build and inject your own "watchpoints" for debugging WebAssembly binaries and how to insert symbols into a stripped binary.

For game hackers, I will show how to use binary instrumentation to implement some old-school game hacking tricks and show off some new ones.

I will be releasing two tools: a binary instrumentation library built for modifying WebAssembly binaries in the browser, and a browser extension that implements common game hacking methods a la Cheat Engine.

## YOUR SECRET FILES ARE MINE: BUG FINDING AND EXPLOIT TECHNIQUES ON FILE TRANSFER APP OF ALL TOP ANDROID VENDORS

Sunday at 10:00 in Track 4  
45 minutes | Demo, Tool, Exploit

**Xiangqian Zhang**  
**Huiming Liu**

Nearby sharing apps are very convenient and fast when you want to transfer files and have been pre-installed on billions of devices. However, we found that most of them will also open a door for

attackers to steal your files and even more.

First, we did a comprehensive research about all top mobile vendors' pre-installed nearby sharing apps by reverse engineering. Many serious vulnerabilities are found on most of them and reported to vendors. Algorithm and design flaws in these apps can lead to file leaking and tampering, privacy leaks, arbitrary file downloads and even remote code execution. We will present all the related vulnerabilities' details and exploit techniques. Next, we conducted the same research on lots of third-party file sharing apps and found that they are even worse about security and are used by surprising more than 1 billion users. Files transferred between them are nearly naked when our MITM attack devices are nearby. Finally, we will summarize all the attack vectors and two common attack models. We will also present the attack demos and related tools.

Besides, we will present our practical mitigations. Currently, we are working with most of the top vendors to mitigate these vulnerabilities. Through this talk, we want to notify users and mobile vendors to pay more attention to this serious situation and fix it better and sooner.

## THE ABC OF NEXT-GEN SHELLCODING

Sunday at 11:00 in Track 1  
45 minutes | Demo, Tool

**Hadrien Barral**

Hacker

**Rémi Géraud-Stewart**

Hacker

**Georges-Axel Jaloyan**

PhD Student at ENS

Shellcodes are short executable stubs that are used in various attack scenarios, whenever code execution is possible. After briefly recalling how they work in general and what interesting things they can do, besides obviously running a reverse-shell, we'll have to deal with the reality that shellcodes are usually not particularly stealthy, due in part to the very suspicious presence of non-printable characters. In a tutorial-like fashion, we'll address increasingly more complex constraints. As a reward, we reveal new methods for writing in particular alphanumeric shellcodes and attacking platforms for which (to the best of our knowledge) no such shellcode was previously known.

Don't know anything about constrained shellcodes? Do not worry: we'll start from the ground up. Black-belt in shellcoding? We have you covered, stay until the end were we'll get our hands dirty!



## SDR AGAINST SMART TVS: URL AND CHANNEL INJECTION ATTACKS

Sunday at 11:00 in Track 2  
45 minutes | Demo, Tool

**Pedro Cabrera Camara**

Founder, Ethon Shield

Software-defined-radio has revolutionized the state of the art in IoT security and especially one of the most widespread devices: Smart TV. This presentation will show in detail the HbbTV platform of Smart TV, to understand and demonstrate two attacks on these televisions using low cost SDR devices: TV channel and HbbTV server impersonation (channel and URL injection). This last attack will allow more sophisticated remote attacks: social engineering, keylogging, crypto-mining, and browser vulnerability assessment.

## EXPLOITING QUALCOMM WLAN AND MODEM OVER THE AIR

Sunday at 11:00 in Track 3  
45 minutes | Demo, Exploit

**Xiling Gong**

Consultant, NCC Group

**Peter Pi**

Senior Security Researcher of Tencent Blade Team

In this talk, we will share our research in which we successfully exploit Qualcomm WLAN in FIRMWARE layer, break down the isolation between WLAN and Modem and then fully control the Modem over the air.

Setup the real-time debugger is the key. Without the debugger, it's difficult to inspect the program flow and runtime status. On Qualcomm platform, subsystems are protected by the Secure Boot and unable to be touched externally. We'll introduce the vulnerability we found in Modem to defeat the Secure Boot and elevate privilege into Modem locally so that we can setup the live debugger for baseband.

The Modem and WLAN firmware is quite complex and reverse engineering is a tough work. Thanks to the debugger, we finally figure out the system architecture, the components, the program flow, the data flow, and the attack surfaces of WLAN firmware. We'll share these techniques in detail, along with the zero-days we found on the attack surfaces.

There are multiple mitigations on Qualcomm baseband, including DEP, stack protection, heap cookie, system call constraint, etc. All the details of the exploitation and mitigation bypassing techniques will be given during the presentation.

Starting from Snapdragon 835, WLAN firmware is integrated into the Modem subsystem as an isolated userspace process. We'll discuss these constraints, and then leverage the weakness we found to fully exploit into Modem.

## SAY CHEESE - HOW I RANSOMWARED YOUR DSLR CAMERA

Sunday at 11:00 in Track 4  
45 minutes | Demo, Exploit

**Eyal Itkin**

Vulnerability Researcher at Check Point Software Technologies

It's a nice sunny day on your vacation, the views are stunning, and like on any other day you take out your DSLR camera and start taking pictures. Sounds magical right? But when you get back to your hotel the real shock hits you: someone infected your camera with ransomware! All your images are encrypted, and the camera is locked. How could that happen? In this talk, we show a live demo of this exact scenario. Join us as we take a deep dive into the world of the Picture Transfer Protocol (PTP). The same protocol that allows you to control your camera from your phone or computer, can also enable any attacker to do that and more. We will describe in detail how we found multiple vulnerabilities in the protocol and how we exploited them remotely(!) to take over this embedded device. But it doesn't end here. While digging into our camera, we found a reliable way to take over most of the DSLR cameras without exploiting any vulnerability at all. We simply had to ask our camera to do that for us, and it worked.

This is the first vulnerability research on the Picture Transfer Protocol, a vendor agnostic logical layer that is common to all modern-day cameras. As DSLR cameras are used by consumers and journalists alike, this opens up the door for future research on these sensitive embedded devices.

## I'M IN YOUR CLOUD... PWINING YOUR AZURE ENVIRONMENT

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

**Dirk-jan Mollema**

Security Expert - Fox-IT

After having compromised on-premise for many years, there is now also the cloud! Now your configuration mistakes can be accessed by anyone on the internet, without that fancy next-gen firewall saving you. With this talk I'll share my current research on Azure privileges, vulnerabilities and what attackers can do once they gain access to your cloud, or how they can abuse your on-premise cloud components. We start with becoming Domain Admin by compromising Azure AD Sync, sync vulnerabilities that allow for Azure admin account takeover and insecure Single Sign On configurations. Up next is cloud roles and privileges, backdooring Azure AD with service accounts, escalating privileges as limited admin and getting past MFA without touching someone's phone. Then we finish with cloud integrations, also known as "how a developer can destroy your whole infrastructure with a single commit": Exploring Azure DevOps, backdooring build pipelines, dumping credentials and compromising Azure Resource Manager through connected services. Besides all the

# PRESENTATIONS

fun we'll also look into how this translates into the questions you should ask yourself before moving things to the cloud and how this differs from on-premise.

## MALPROXYING: LEAVE YOUR MALWARE AT HOME

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

**Hila Cohen**

Security Researcher, XM Cyber

**Amit Waisel**

Senior Technical Leader, XM Cyber

During a classic cyber attack, one of the major offensive goals is to execute code remotely on valuable machines. The purpose of that code varies on the spectrum from information extraction to physical damage. As defenders, our goal is to detect and eliminate any malicious code activity, while hackers continuously find ways to bypass the most advanced detection mechanisms. It's an endless cat-and-mouse game where new mitigations and features are continuously added to the endpoint protection solutions and even the OS itself in order to protect the users against newly discovered attack techniques. In this talk, we present a new approach for malicious code to bypass most of endpoint protection measures. Our approach covertly proxies the malicious code operations over the network, never deploying the actual malicious code on the victim side. We are going to execute code on an endpoint, without really storing the code on disk or loading it to memory. This technique potentially allows attackers to run malicious code on remote victims, in such a way that the code is undetected by the victim's security solutions. We denote this technique as "malproxying".

## HTTP DESYNC ATTACKS: SMASHING INTO THE CELL NEXT DOOR

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

**albinowax**

Head of Research, PortSwigger

HTTP requests are traditionally viewed as isolated, standalone entities. In this session, I'll introduce techniques for remote, unauthenticated attackers to smash through this isolation and splice their requests into others, through which I was able to play puppeteer with the web infrastructure of numerous commercial and military systems, rain exploits on their visitors, and harvest over \$50k in bug bounties.

Using these targets as case studies, I'll show you how to delicately amend victim's requests to route them into malicious territory, invoke harmful responses, and lure credentials into your open arms. I'll also demonstrate using backend reassembly on your own requests to exploit every modicum of trust placed on the frontend, gain maximum privilege access to internal APIs, poison web caches, and compromise my favourite login page.

Although documented over a decade ago, a fearsome reputation for difficulty and collateral damage has left this attack optimistically ignored for years while the web's susceptibility grew. By applying fresh ideas and new techniques, I'll unveil a vast expanse of vulnerable systems ranging from huge content delivery networks to bespoke backends, and ensure you leave equipped to devise your own desync techniques and tailor attacks to your target of choice.

## HELP ME, VULNERABILITIES. YOU'RE MY ONLY HOPE

Sunday at 12:00 in Track 4  
45 minutes | Tool, Exploit

**Jacob Baines**

Research Engineer, Tenable

MikroTik routers keep getting owned. They've been exploited by advanced threats like VPNFilter, Slingshot APT, and Trickbot. They've been compromised by coin miners, botnets, and who knows what else. With each new campaign the security industry publishes new indicators of compromise and everyone moves on.

However, MikroTik administrators operate in a sandbox. They have very limited access to the router's underlying file system and almost no ability to directly interact with the Linux operating system. Due to these limitations, file hashes cannot answer the fundamental question that is asked again and again on the MikroTik forums, "Have I been compromised?"

It's time the users had their question answered. In this talk, I'll present three vulnerabilities that can help MikroTik administrators break out of the sandbox. I'll show how to use these vulnerabilities to help determine if the router has been compromised.

## [ MI CASA-SU CASA ] MY 192.168.1.1 IS YOUR 192.168.1.1

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

**Elliott Thompson**

Senior Security Consultant, SureCloud Ltd

Your browser thinks my 192.168.1.1 is the same as your 192.168.1.1. Using a novel combination of redirects, Karma, JavaScript and caching we demonstrate that it's viable to attack internal management interfaces without ever connecting to your network. Using the MICASA-SUCASA tool it's possible to automate the exploitation of hundreds of interfaces at once. This presentation will introduce the attack vector and demonstration, but also the public release of the MICASA-SUCASA tool.



## SOUND EFFECTS: EXPLORING ACOUSTIC CYBER-WEAPONS

Sunday at 13:00 in Track 2  
45 minutes | Tool

**Matt Wixey**

Cyber Security Research Lead, PwC UK

While recent research has explored the capability of attacks to cause harm by targeting devices—e.g., SCADA systems, vehicles, medical implant devices—little consideration has been given to the concept of attacks affecting psychological and physiological health by targeting humans themselves.

In a first-of-its-kind study, we assessed the capability of several consumer devices to produce sound at high and low frequencies which may be imperceptible to many people, as a result of remote and local attacks, and compared the resulting sound levels to maximum recommended levels. In doing so, we tested their viability as localised acoustic weapons which could cause temporary/permanent hearing damage and/or adverse psychological effects. We examined a number of countermeasures, including a tool to detect specified frequencies above specified thresholds.

In this talk, I will cover the background of malware which has, intentionally or not, caused physical or psychological harm. I will explore previous research on the harmful effects of sound, focusing particularly on high and low frequencies, and some of the guidance which has been proposed to limit exposure to such sound. I will examine the use of imperceptible sound as applied to security research (covert channels, ultrasonic tracking beacons, etc), and will present our experiments and findings, including threat models, methodology, the attacks we developed, and the implications of our results. Finally, I will suggest a number of countermeasures and outline some possible areas for future research.

## OWNING THE CLOUD THROUGH SERVER-SIDE REQUEST FORGERY

Sunday at 13:00 in Track 3  
45 minutes | Demo, Tool

**Ben Sadeghipour**

Nahamsec

**Cody Brocious (Daeken)**

With how many apps are running in the cloud, hacking these instances becomes easier with a simple vulnerability due to an unsanitized user input. In this talk, we'll discuss a number of different methods that helped us exfil data from different applications using Server-Side Request Forgery (SSRF). Using these methods, we were able to hack some of the major transportation, hospitality, and social media companies and make \$50,000 in rewards in 3 months.

## WANT STRONG ISOLATION? JUST RESET YOUR PROCESSOR

Sunday at 13:00 in Track 4  
20 minutes | Demo, Tool

**Anish Athalye**

PhD student at MIT

Today's systems sandbox code through traditional techniques: memory protection and user-kernel mode. Even high-security devices like hardware cryptocurrency wallets use such an architecture. Unfortunately, this arrangement has a history of security bugs due to misconfigured protection hardware, bugs in kernel code, hardware bugs, and side channels.

This talk proposes a new approach to isolation for devices like crypto wallets: separate the user and kernel onto two CPUs and multiplex processes by completely resetting the user processor between tasks so that there is no leakage.

Processor reset is more complicated than might be expected. Simply asserting the reset line isn't enough to clear all CPU-internal state, but it turns out that software can be used to clear this state. However, reasoning about the correctness of such code is challenging. This talk presents a tool that can be used to develop and formally verify the correctness of reset code for a given CPU implementation.

This talk also walks through a design of a wallet based on this reset-based isolation technique, discusses known security vulnerabilities in current designs such as the Ledger and Trezor wallets (including bugs in MPU misconfiguration, system calls, and drivers), and explores how a reset-based design could prevent such vulnerabilities.

## FIRMWARE SLAP: AUTOMATING DISCOVERY OF EXPLOITABLE VULNERABILITIES IN FIRMWARE

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

**Christopher Roberts**

DARPA's Grand Cyber Challenge foretold an ominous future stricken with machines exploiting our code and automatically compromising our systems. Today, we have the chance to steel ourselves by creating new hope through stronger tools and techniques to find our bugs before our big-brother nationstates can take advantage. The firmware holding our phones, our routers, and our cars is our weakest link and it demands new methods of finding exploitable vulnerabilities. This talk will present Firmware Slap, the culmination of concolic analysis and semi-supervised firmware function learning. Each binary or library in a given firmware provides slices of information to accelerate and enable fault-resistant concolic analysis. These techniques provide a method of knowing where our vulnerabilities are and how we can trigger them.

## CHEATING IN ESPORTS: HOW TO CHEAT AT VIRTUAL CYCLING USING USB HACKS

Sunday at 14:00 in Track 2  
45 minutes | Demo, Tool

**Brad Dixon**

Security Consultant, Carve Systems

Athletes are competing in virtual cycling by riding real bikes on stationary trainers which power the in-game athletic performance. Riders train and compete online against each other. New racing teams are even competing in Union Cycliste Internationale (UCI) sanctioned events. Better at hacking than riding? Me, too. I'll expand on the dubious achievements of prior cycling cheaters by showing how to use the open source USBQ toolkit to inspect and modify USB communications between the Zwift application and the wireless sensors that monitor and control the stationary trainer. USBQ is a Python module and application that uses standard hardware, such as the Beaglebone Black, to inspect and modify communications between USB devices and the host. You'll ride away with a lesson on building your own customized USB man-in-the-middle hacking tool, too.

## THE ETHER WARS: EXPLOITS, COUNTER-EXPLOITS AND HONEYPOTS ON ETHEREUM

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

**Bernhard Mueller**

ConsenSys Diligence

**Daniel Luca**

Ethereum smart contracts are Turing-complete programs that mediate transfers of money. It doesn't come as a surprise that all hell is breaking loose on the Ethereum blockchain.

In this talk, we'll introduce Karl, an Ethereum blockchain monitor, and Scrooge McEthereface, an auto-exploitation bot that extracts Ether from vulnerable smart contracts. Scrooge uses symbolic execution to detect vulnerable states that live up to three transactions deep and constructs exploit payloads using the Z3 constraint solver.

We'll also examine the game-theoretic consequences of Scrooge's existence. What if multiple bots compete for exploiting the same contracts? How about honeypots that counter-exploit bots? Is it possible to cheat those honeypots? When all is said and done, who is going to end up stealing money from whom?

During the talk, we'll show many examples for vulnerable contracts, honeypots, and counter-honeypots, explain the role of transaction ordering and frontrunning, and launch a little challenge for the audience.

## CONTESTS AWARDS CEREMONY

Sunday at 14:00 in Track 4  
90 minutes

### Contests & Events

You've seen the Contests, you've played in a Contest, you've won a Contest and may have lost a Contest! Whatever the outcome was, come join as we celebrate the winners and contestants of our DEF CON 27 Contests! DEF CON 27 Contests and Events Closing Ceremonies will be August 11th at 14:00 in Track 4. Black Badge winning Contests will still be honored at the main DEF CON 27 Closing Ceremonies on August 11th at 16:00 in the Paris Ballroom!

## CLOSING CEREMONIES

Sunday at 16:00 in Paris Ballroom  
120 minutes

### The Dark Tangent & Goons

DEF CON 27 draws to a close. Prizes awarded, Black Badge winners announced, thanks given, future plans revealed.

## "FIRST-TRY" DNS CACHE POISONING WITH IPV4 AND IPV6 FRAGMENTATION

Backup at 00:00 in 0  
45 minutes | Demo, Exploit

**Travis (Travco) Palmer**

Security Research Engineer, Cisco

**Brian Somers**

Site Reliability Engineer

DNS fragmentation attacks are a more recent series of attacks that take advantage of the consistent composition of fragmented DNS responses by sending a crafted (malicious) second fragment to be reassembled with a legitimate first fragment at the IP layer. Even if DNSSEC is fully implemented, an attacker can still poison unsigned "glue" records.

These types of attacks are difficult, and have really only been considered remotely feasible over IPv4. Most nameservers use "per-destination" IP-layer ID (IPID) counters, and the IPID in the IPv6 Fragment Extension Header cannot be easily guessed blindly, as the number of bits in the field has been comparatively doubled to 32 bits (making blind-guessing even in ideal conditions take an average 34 million iterations).

Unfortunately, as part of optimizations made to Linux. The IPID counter is no longer truly "per-destination" and the IPID for a given destination can be inferred consistently enough to facilitate an attack. This allows DNS poisoning on IPv4 and IPv6 with equal consistency and precision, and makes poisoning on the first attempt "thousands" of times easier.

This talk will cover how this attack is carried out, how consistent it really can be, and mitigations that can be put in place by operators of both DNS nameservers and resolvers to limit its effectiveness.



# SKYTALKS

LOCATION: PACIFIC BALLROOM, BALLY'S JUBILEE TOWER, 2ND FLOOR

SINCE 2008, WE HAVE BEEN BRINGING YOU OLD-SCHOOL DEFCON: TECHNICAL DEEP DIVES, NO HOLDS BARRED DISCUSSIONS, COOL TECHNOLOGY, EARLY-ACCESS TALKS, AND PLENTY OF SHENANIGANS.

"NO RECORDING. NO PHOTOGRAPHS. NO BULLSHIT!"

THIS IS HOW WE ROLL.

THE ENTIRE SKYTALKS ROOM IS "OFF-THE-RECORD" AND FOR THE SAFETY OF OUR PRESENTERS, WE HAVE A NO ELECTRONICS AND NO REPORTING POLICY. WE FEEL THAT THIS ENCOURAGES A MORE INTIMATE AND COLLEGIAL ATMOSPHERE. WE ENCOURAGE INTERACTION AND DISCUSSION WITH OUR SPEAKERS, AND WE ENCOURAGE THEM TO BE CREATIVE WITH THEIR TALKS.

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

FOR UP-TO-DATE INFORMATION PICK UP  
A SCHEDULE AT THE JUBILEE BALLROOMS  
OR DEF CON INFO BOOTHS.

ALSO AVAILABLE ON:  
TWITTER (@DCSKYTALKS)  
HACKER TRACKER  
[HTTPS://SKYTALKS.INFO/](https://skytalks.info/)

SKYTALKS 2019 DEDICATED TO TUNA

# DEMO LABS

## ANTENNAS FOR SURVEILLANCE APPLICATIONS

Friday from 10:00 – 11:50 in Sunset 1 at Planet Hollywood

Audience: All

**Kent Britain & Alexander Zakharov**

The antenna is one of the most important pieces of a good receiver. Yet it seems technical specifications are made up by the Marketing Departments, not by the Engineers. Wild claims about gain and misleading data seem to be the norm. In this Demonstration you will be able to see and hear the effects of gain and have a better understanding of beamwidths and patterns. Over a dozen different antennas will be available for demonstration, and our miniature antenna range can do some quick tests on your antenna.

<http://WWW.WA5VJB.COM>

## BEDR

Saturday from 12:00 – 13:50 in Sunset 6 at Planet Hollywood

Audience: Defense, Linux

**Mark Ignacio**

bedr is a Linux syscall monitor that uses Berkeley Packet Filters that hook via kernel tracepoints. It collects the holy trinity of EDR data - proc events, filemods, and netconns - and ships them off to somewhere else for off-machine detection and response. Basically, it's half of what you need to make an EDR!

<https://github.com/mark-ignacio/bedr>

## BEEKMA – ELECTRON POST-EXPLOITATION FRAMEWORK

Friday from 10:00 – 11:50 in Sunset 3 at Planet Hollywood

Audience: Offense – Especially red teamers that want to establish persistence and egress data.

**Pavel Tsakalidis**

BEEKMA is a tool that allows Red-Teamers to establish persistence on a compromised host, or even egress data from the it. In addition, it allows them to execute code from within the context of the compromised application (Slack, Skype, WhatsApp, Bitwarden, VS Code) allowing them to access otherwise inaccessible data. Come find out how you can extract all passwords from Bitwarden, or how to egress all the source code files from VS Code!

<https://github.com/ctxis/beemka/>

## BURPSUITE TEAM SERVER FOR COLLABORATIVE WEB APP TESTING

Saturday from 14:00 – 15:50 in Sunset 1 at Planet Hollywood

Audience: Offense, AppSec

**Tanner Barnes**

During large scale engagements against multiple applications teams often split the workload across many testers. Currently, sharing Burpsuite states requires

exporting large files that are point in time requiring multiple exports and shares if new developments in engagement occur which restricts the ability for teams to collaborate on an application. With my new Bursuite plugin, coupled with a lightweight server, multiple testers can share traffic in real time across multiple applications allowing for quick collaboration! Have a repeater payload your team needs to see? Simply right click the request and select share to populate their repeater tabs! Need help with a intruder payload? Have another tester create it and send it to you! Come listen and see how this plugin can help your teams hack collaboratively!

<https://github.com/Static-Flow/BurpSuite-Team-Extension>

## CHAOS DRIVE, BECAUSE USB IS STILL TOO TRUSTWORTHY

Friday from 14:00 – 15:50 in Sunset 4 at Planet Hollywood

Audience: Offense, Social Engineers, Hardware, Privacy

**Mike Rich**

If you've never thought USB devices could become even less trustworthy, then this is the talk for you. We already know USB devices might try to automatically run code when connected, or act like a hyperactive keyboard and mouse, or attempt to physically destroy the host, or masquerade as an innocent charging/data cable. But it can, actually, get worse. Say hello to the Chaos Drive, a USB drive with just a little too much chaotic energy. I'll demonstrate how a Linux-based USB mass storage device can be set up to change the storage it presents to the host based on a set of user-defined conditions. On the offensive side this can be used to circumvent USB scanning procedures and on the defensive side this can be used to store private files that will be undetectable without time-consuming analysis. Attendees will learn the steps I took to build the POC and see what it can do. For best results bring a USB OTG-capable device such as a Pi Zero or Pocketbeagle, an OTG cable, and some spare microSD cards to flash.

## CIRCO: CISCO IMPLANT RASPBERRY CONTROLLED OPERATIONS

Saturday from 10:00 – 11:50 in Sunset 2 at Planet Hollywood

Audience: Offense, Hardware

**Emilio Couto**

Designed under Raspberry Pi and aimed for Red Team Ops, we take advantage of "Sec/Net/Dev/Ops" enterprise tools to capture network credentials in a stealth mode. Using a low-profile hardware & electronics camouflaged as simple network outlet box to be sitting under/over a desk. CIRCO include different techniques for network data exfiltration to avoid detection from IDS/IPS or monitoring systems. This tool gathers information and use a combination of honeypots to trick Automation Systems to give us their network credentials! We will build a physical network & infrastructure lab to show how CIRCO works (live demo) Major features for release v1.5 (Aug):

- Allow existing IP-Phone to co-exist with CIRCO



- Eliminate template files (craft all packets)
- Support NTP exfiltration
- Software encrypted via Bluetooth (prevent forensic)
- Self destroy and alarm switch
- Bypass active & passive fingerprinting (NAC)
- Credentials integration into Faraday

<https://github.com/ekiojp/circo>

## COMBO PASSWORD

Friday from 14:00 – 15:50 in Sunset 5 at Planet Hollywood

Audience: Defense

### Fabian Obermaier

Combo Password is a PoC for using (as the name suggests) key combinations in passwords. There is one nice implication that might justify the increased complexity and other possible gripes: Compared to a normal password, a combo password of the same length has far more possible combinations. This effect is increasing with password length and the number of usable keys. With three available keys and a length of two there are 9 combinations for normal passwords and 15 for combo passwords. Increasing the length to three we get 27 vs 69 combinations. This could lead to less strict password requirements while increasing the security. The goal of this project is to develop a free standard, a browser plugin for using combo passwords in regular login forms and implementations for popular languages, frameworks and PAM. Visit Demo Labs and try to break a real hackers password, there will be a small reward for the fastest brute force tool!

<http://combo-pw.tech/>

<https://gitlab.com/FalkF/combopassword>

## COTOPAXI: IOT PROTOCOLS SECURITY TESTING TOOLKIT

Saturday from 10:00 – 11:50 in Sunset 3 at Planet Hollywood

Audience: IoT, AppSec

### Jakub Botwicz

Cotopaxi is a set of tools for security testing of Internet of Things devices using specific network IoT/IoT/M2M protocols (e.g. CoAP, MQTT, DTLS, mDNS, HTCPCP). These tools will be used by penetration testers or security researchers to identify IoT services and verify security vulnerabilities or misconfigurations. Currently available tools used for security testing, like nmap or OpenVAS, do not support all new IoT protocols. So possibilities to test IoT products and discover such devices in tested networks are limited. We are working to fill this gap with Cotopaxi toolkit. Main features of our toolkit are:

- Checking availability of network services for supported IoT protocols at given IPs and port ranges ("service ping")
- Recognizing the software used by remote network server ("IoT software fingerprinting") based on responses for given messages using machine learning classifier

- Discovering resources identified by given URLs ("dirdusting")

- Performing black-box fuzzing of IoT protocols based on corpus of packets prepared using coverage-based fuzzer

- Identifying known vulnerabilities in IoT servers

- Detecting network traffic amplification.

New features in release for DEF CON27 are:

- client-side versions of protocol fuzzer and vulnerability tester

- support for new protocols: SSDP and HTCPCP.

<https://github.com/Samsung/cotopaxi>

## BURP PLUGIN: CYBER SECURITY TRANSFORMATION CHEF (CSTC)

Saturday from 12:00 – 13:50 in Sunset 1 at Planet Hollywood

Audience: Offense, Defense, AppSec, Mobile.

### Ralf Almon & Sebastian Puttkammer

CSTC is a Burp Suite extension for various input transformations. It implements a generic solution that can replace numerous specialized extensions. The CSTC solves the problem of having too specific burp plugins by being a more generic problem solving tool. It contains a wide range of very simple operations that can be chained into complex transformations. This allows a penetration tester to create the exact transformation they need to test a specific product without having to write any code. As we all know, writing code and setting everything up is time consuming. You can configure complex input transformations for both requests and responses simply by using drag and drop. You can calculate HMACs for parts of the request, refresh timestamps, update sequence numbers or encrypt parts of the request. You can chain together different operations to create more complex transformations. You could extract parts of the request, decompress them, insert your payload using the repeater or utilizing the scanner and put it back in and compress it again before sending it. Since there are already many basic operations implemented, you can easily focus on testing the application instead of searching for extensions performing such transformations.

<https://github.com/usdag/cstc>

## DR.ROBOT: ORGANIZED CHAOS AND THE SHOTGUN APPROACH

Saturday from 12:00 – 13:50 in Sunset 5 at Planet Hollywood

Audience: Defense/Offense

### Aleksandar Straumann & Jayson Grace

Companies are large, and the number of subdomains they expose is even larger. There are a number of tools to uncover subdomains an organization is exposing, but individually they do not give you the complete picture. In the event that you use multiple tools, you are given an overwhelming amount of data to piece together into an aggregate view. In this talk we introduce Dr.ROBOT,

# DEMO LABS

a domain reconnaissance tool that was developed to run a large variety of subdomain enumeration tools. It was designed to trivially incorporate new tools as they are released by leveraging Docker and Ansible. Dr.ROBOT has three stages: gathering, inspection, and publishing. In the gathering stage, it gathers as much information as it can and aggregates the results. In the inspection phase, it captures screenshots and other information regarding the target. Finally, in the publishing phase it sends the data gathered during the previous two phases to an endpoint for manual review. Dr.ROBOT was created to serve as a comprehensive source on subdomain exposure by gathering information from as many resources as possible. It is a versatile utility for bug bounty hunters, blue teams, red teams, and many others.

[https://github.com/sandialabs/dr\\_robot](https://github.com/sandialabs/dr_robot)

## EAPHAMMER

Friday from 12:00 - 13:50 in Sunset 1 at Planet Hollywood

Audience: Offensive security professionals, security analysts and network administrators, executive leadership, end-users

### Gabriel Ryan

EAPHammer is a toolkit for performing targeted rogue access point attacks against enterprise wireless infrastructure. It is designed to be used in full scope wireless assessments and red team engagements. As such, focus has been placed on providing an easy-to-use interface that can be leveraged to execute powerful wireless attacks with minimal manual configuration.

This summer will mark the third anniversary of EAPHammer since it was released at DEF CON Demo Labs and BlackHat Arsenal in 2017. It's also the most exciting and complete version of the tool yet, with the addition of a number of features that were requested directly by users at Demo Labs in 2018.

EAPHammer now supports most of the bleeding edge attacks that have been discovered by the wireless community over the past few years, including:

- WPA3 Transition Mode and Security Group Downgrade Attacks
- Reflection and Invalid Curve attacks against EAP-pwd
- GTC-Downgrade, Fixed Challenge, and EAP Relay attacks against WPA/2-EAP
- PMKID attacks against WPA/2-PSK networks
- Known Beacons Attack and Legacy SSL Support
- External Certificate Handling and Import

Perhaps most excitingly, we've also included some never-before-seen attacks against Opportunistic Wireless Encryption (OWE), which is better known as "Enhanced Open".

<https://github.com/s0l3t1ce/eaphammer>

## EXPLIOT - IOT SECURITY TESTING AND EXPLOITATION FRAMEWORK

Friday from 14:00 - 15:50 in Sunset 3 at Planet Hollywood

Audience: Offense, Hardware, IoT, Pentesters

### Aseem Jakhar & Murtuja Bharmal

EXPLIoT is a framework for security testing and exploiting IoT products and IoT infrastructure. Source code and documentation - [https://gitlab.com/exploit\\_framework/exploit](https://gitlab.com/exploit_framework/exploit) It provides a set of plugins (test cases) which are used to perform the assessment and can be extended easily with new ones. The name EXPLIoT (pronounced expl-aa-yo-tee) is a pun on the word exploit and explains the purpose of the framework i.e. IoT exploitation. It can be used as a standalone tool for IoT security testing and more interestingly, it provides building blocks for writing new plugins/exploits and other IoT security assessment test cases with ease. EXPLIoT supports most IoT communication protocols, 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. Currently, the framework has support for analyzing and exploiting various IoT, radio and hardware protocols including BLE, CAN, DICOM, MQTT, Modbus, I2C, SPI, UART We have released a comprehensive documentation including User and Developer guide to help the security community kick start quickly and easily with the framework.

[https://gitlab.com/exploit\\_framework/exploit](https://gitlab.com/exploit_framework/exploit)

## FLATLINE

Friday from 12:00 - 13:50 in Sunset 4 at Planet Hollywood

Audience: Hardware and OpSec

### East

Flatline is a deterministic hardware credential manager. It can generate passwords, burner accounts, shortlinks, and BIP39 seeds. Based on a single mnemonic seed, with Flatline it is possible to store millions of dollars in cryptocurrency, and shortlinks that map to sensitive or stolen data. Store a criminal empire in your head, maintain a map of leaked documents that are hosted on the internet while storing nothing on your local disk, or maintain access to your assets when your house burns down and you have to flee to eastern Europe.

<https://gitlab.com/e4st/flatline>

## GO REVERSE ENGINEERING TOOL KIT

Saturday from 10:00 - 11:50 in Sunset 5 at Planet Hollywood

Audience: Defense

### Joakim Kennedy

The Go Reverse Engineering Tool Kit (go-re.tk) is a new open-source toolset for analyzing Go binaries. The tool is designed to extract as much metadata as possible from stripped binaries to assist in both reverse engineering and malware analysis. For example, GoRE can detect the compiler version used, extract type



information, and recover function information, including source code line numbers for functions and source tree structure. The core library is written in Go, but the tool kit includes C-bindings and a library implementation in Python. When using the C-bindings or the Python library, it is possible to write plugins for other analysis tools such as IDA Pro and Ghidra. The toolset also includes "redress", which is a command line tool to "dress" stripped Go binaries. It can both be used standalone to print out extracted information from the binary or as a radare2 plugin to reconstruct stripped symbols and type information. The tool kit consists of:

- \* Core library written in Go
- \* C-bindings
- \* Python library using the C-bindings
- \* A command line tool for easy analysis

<https://github.com/goretk>

## HACHI: AN INTELLIGENT THREAT MAPPER

Friday from 10:00 – 11:50 in Sunset 5 at Planet Hollywood

Audience: Defense, Malware, Threat Intelligence

### Parmanand Mishra

ATT&CK framework has become a benchmark in the security domain. ATT&CK provides data about each technique used across different attack stages. Hachi was created to contribute to the ATT&CK community. Hachi is based on the radare2 framework and uses data provided by ATT&CK to map the symptoms of malware on ATT&CK matrix.

Following modules of Hachi make this tool a great addition to an analyst's or company's armaments:

- Threat Intel: Hachi provides threat intelligence data like a possible parent campaign or author of a malware file.
- Malware behavior: It uncovers core malware behaviors using automated static analysis coupled with symbolic execution to explore multiple execution paths and maps it on ATT&CK matrix.
- RESTful API: Hachi provides RESTful API which enables this tool to seamlessly integration with malware processing frameworks.
- Visualization: It allows for the creation of detailed visual reports.
- Integration with Threat Intel feeds: It can be integrated with different threat intelligence feeds for enhanced security or expanded insights.

The primary aim of this tool is to act as a force multiplier for the InfoSec community and aid the analysis of malware.

<https://github.com/Kart1keya/Hachi>

Browser extension to hunt low hanging fruits (Hacking by just browsing)

Friday from 14:00 – 15:50 in Sunset 1 at Planet Hollywood

Audience: Bug bounty hunters, Penetration testers, developers, open source contributors

Rewanth Cool

Automated scanners won't yield you bugs these days. They take tens of hours to get completed and with too with a high false rate. You need a minimal smart scanner with easy installation, easy configuration, and relatively high accuracy while hunting for bugs. This talk is focused on creating such a browser extension to yield better results in less time. The browser extension requires less manual effort and produces more accurate results in just a few seconds.

<https://github.com/rewanth1997/vuln-headers-extension>

## IOC2RPZ

Saturday from 12:00 – 13:50 in Sunset 2 at Planet Hollywood

Audience: Defense

### Vadim Pavlov

DNS is the control plane of the Internet with unprecedented detailed views on applications, devices and even transferred data going in and out of a network. 80% of malware uses DNS to communicate with Command & Control for DNS data exfiltration/infiltration and phishing attacks using lookalike domains. Response Policy Zones or DNS Firewall is a feature which allows us to apply security policies on DNS. Commercial DNS Firewall feeds providers usually do not allow user to generate their own feeds. Cloud only DNS service provides do not provide feeds for on-prem DNS. ioc2rpz is a DNS server which automatically creates, maintains and distributes DNS Firewall feeds from various local (files, DB) and remote (http, ftp, rpz) sources. This enables easy integrations with Threat Intel providers and Threat Intelligence Platforms. The feeds can be distributed to any open source and commercial DNS servers which support RPZ, e.g. ISC BIND, PowerDNS, Infoblox, BlueCat, Efficient IP etc. With ioc2rpz you can create your own feeds, actions and prevent undesired communications before they happen.

<http://ioc2rpz.com>

## LET'S MAP YOUR NETWORK

Friday from 14:00 – 15:50 in Sunset 2 at Planet Hollywood

Audience: Defense, Monitoring

### Pramod Rana

Let's Map Your Network (LMYN) aims to provide an easy to use interface to security engineer and network administrator to have their network in graphical form with zero manual error. It is utmost important for any security engineer to understand their network first before securing it. In a mid to large level organisation's network having a network architecture diagram doesn't provide the complete understanding and manual verification is a nightmare. Hence in order to secure entire network it is important to have a complete picture of all the systems which are connected to your network, irrespective of their type, function, technology etc. **BOTTOM LINE - YOU CAN'T SECURE WHAT YOU ARE NOT AWARE OF.** LMYN does it in two phases:

1. Learning: In this phase LMYN 'learns' the network by performing the network commands and querying the APIs and then builds graph database

# DEMO LABS

leveraging the responses. User can perform any of the learning activities at any point of time and LMYN will incorporate the results in existing database.

2. Monitoring: This is a continuous process, where LMYN monitors the 'in-scope' network for any changes, compare it with existing information and update the graph database accordingly.

<https://github.com/varchashva/LetsMapYourNetwork>

## LOCAL SHERIFF

Saturday from 12:00 – 13:50 in Sunset 3 at Planet Hollywood

Audience: AppSec, Code Assessments, and privacy researchers

### Konark Modi

URL is the most commonly tracked piece of information, the innocent choice to structure a URL based on page content can make it easier to learn a users' browsing history, address, health information or more sensitive details. While you as a user normally browse the internet Local Sheriff works in the background and helps you identify what sensitive information(PII—Name, Date Of Birth, Email, Passwords, Passport number, Auth tokens.) is being shared/leaked to which all third-parties and by which all websites. The issues that Local Sheriff helps identify:

- What sensitive information is being shared with whom?
- Which companies are own these third parties?
- What can they doing with this information? EG: de-anonymize users on the internet, create shadow profiles.
- Data points that can be used for tracking a user across the web.
- Insights into which companies know what about you on the internet.

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 browser extension that can used with Chrome, Opera, Firefox, Brave, Cliqz.

<https://github.com/cliqz-oss/local-sheriff/tree/master/scripts>

## MEMHUNTER - AUTOMATED HUNTING OF MEMORY RESIDENT MALWARE AT SCALE

Saturday from 10:00 – 11:50 in Sunset 6 at Planet Hollywood

Audience: Defense

### Marcos Oviedo

Memhunter is an endpoint sensor tool specialized in detecting memory-resident malware. The detection process is performed through a combination of endpoint data collection and memory inspection scanners. The tool is a standalone binary that, upon execution, deploys itself as a windows service. Once

running as a service, memhunter starts the collection of ETW events that might indicate code injection attacks. The live stream of collected data events is feed into memory inspection scanners that use detection heuristics to down select the potential attacks. The entire detection process does not require human intervention, neither memory dumps, and it can be performed by the tool itself, at scale, improving the threat hunting analysis process and remediation times. The tool was designed as a replacement of memory forensic mechanisms such as volatility malfind and hollowfind plugins, which requires human analysis and memory dumps to find suspicious artifacts on memory. Besides the data collection and hunting heuristics, the project has also led to the creation of a companion tool called minjector that contains +20 code injection techniques. The minjector tool can be used to exercise memhunter detections, and as a one-stop learning solution on well-known code injection techniques out there.

<https://github.com/marcosd4h/memhunter>

OSfooler-NG: Next Generation of OS fingerprinting fooler

Friday from 14:00 – 15:50 in Sunset 6 at Planet Hollywood

Audience: Defense

Jaime Sanchez

An outsider has the capability to discover general information, such as which operating system a host is running, by searching for default stack parameters, ambiguities in IETF RFCs or non-compliant TCP/IP implementations in responses to malformed requests. By pinpointing the exact OS of a host, an attacker can launch an educated and precise attack against a target machine. There are lot of reasons to hide your OS to the entire world: Revealing your OS makes things easier to find and successfully run an exploit against any of your devices. Having an unpatched or antique OS version is not very convenient for your company prestige. Imagine that your company is a bank and some users notice that you are running an unpatched box. They won't trust you any longer! In addition, these kind of 'bad' news are always sent to the public opinion. Knowing your OS can also become more dangerous, because people can guess which applications are you running in that OS (data inference). For example if your system is a MS Windows, and you are running a database, it's highly likely that you are running MS-SQL. It could be convenient for other software companies, to offer you a new OS environment (because they know which you are running). And finally, privacy; nobody needs to know the systems you've got running. OSfooler was presented at Blackhat Arsenal 2013. It was built on NFQUEUE, an iptables/ip6tables target which delegate the decision on packets to a userspace. It transparently intercepted all traffic that your box was sending in order to camouflage and modify in real time the flags in TCP/IP packets that discover your system. OSfooler-NG has been complete rewritten from the ground up, being highly portable, more efficient and combining all known techniques to detect and defeat at the same time: Active remote OS fingerprinting: like Nmap Passive remote OS fingerprinting: like p0f v2 Commercial engines like Sourcefire's FireSIGHT OS fingerprinting Some additional features are: No need for kernel modification or patches Simple user interface



and several logging features Transparent for users, internal process and services Detecting and defeating mode: active, passive & combined Will emulate any OS Capable of handling updated nmap and p0f v2 fingerprint database Undetectable for the attacker  
<https://github.com/segofensiva/OSfooler-ng>

## OWASP AMASS

Saturday from 14:00 – 15:50 in Sunset 2 at Planet Hollywood

Audience: Red Team, Blue Team, Bug Bounty Hunters, Penetration Testers

### Jeff Foley & Anthony Rhodes

Today, organizations deal with the challenge of running their infrastructure across many networks and namespaces due to the use of cloud and hosting services, legacy environments and acquisitions. This can make it difficult for an organization to maintain visibility of its Internet-facing assets and an ability to track down systems that pose a risk to its security posture. The OWASP Amass Project has developed a tool to help information security professionals perform network mapping of attack surfaces and perform external asset discovery. During this talk, contributors to the project will discuss how OWASP Amass uses OSINT, network reconnaissance, graph databases and information sharing to provide both attackers and defenders better visibility of target organizations. Presenters will be providing an in-depth tour of all OWASP Amass features with tips and tricks shown along the way.

<https://github.com/OWASP/Amass>

## PCAPXRAY

Friday from 12:00 – 13:50 in Sunset 2 at Planet Hollywood

Audience: Defense, Forensics, Networks

### Srinivas Piskala Ganesh Babu

PcapXray is a Network Forensics tool that performs pcap visualization to help/speed up traffic investigation offline. [ in n00b terms, Draws a Network Map and Highlights what needs to be looked for in a packet capture. ]

- \* Creates visual drawing (map) of a pcap file and highlights/extracts details for faster/robust traffic forensics/analysis
  - \* Reverse Engineer a Pcap [Packet Capture] File ( Wireshark always is the best goto ), PcapXray plays as a sidecar to speed things up with the investigation ( where/what to look at/for? )
  - \* Promote navigation of a packet capture
  - \* Accomplish Simple goal In the best way ( I could not easily find an offline tool to draw/map/ highlight a pcap file ) -> [ Just for Security Fun! ]
- Capabilities include
- \* Converting a packet capture into a diagram/graph/visual representation
  - \* Segregating and filtering with respect to traffic type, the current list includes HTTP, HTTPS, Tor, Possible Malicious, ICMP, DNS
  - \* Extracting payload and present

traffic on a session/flow basis

- \* Enriching the traffic data with host scans to generate Reports
- \* Identifying covert communication and possibility to extract files included in the traffic

<https://github.com/Srinivas11789/PcapXray>

## PCILEECH AND MEMPROCFS

Saturday from 12:00 – 13:50 in Sunset 4 at Planet Hollywood

Audience: Offense, Defense, Forensics, Hardware

### Ulf Frisk & Ian Vitek

PCILeech and MemProcFS: The PCILeech direct memory access attack toolkit was presented at DEF CON 24 and quickly became popular amongst red teamers, governments and game cheaters alike. We will demonstrate how to take total control of still vulnerable systems with PCIe DMA code injection using affordable FPGA hardware and the open source PCILeech direct memory access attack toolkit. MemProcFS - The Memory Process File System is memory forensics and analysis made super easy! Analyze memory by clicking on files in a virtual file system or by using the C and Python API. A wide range of memory acquisition methods are supported. Analyze memory dump files by point and click, analyze live memory acquired using PCILeech PCIe FPGA hardware devices or even live memory acquired in real time from remote hosts over the network. Zero-cost open source memory forensics and incident response?

<https://github.com/ufrisk/pcileech> <https://github.com/ufrisk/MemProcFS>

## PHANTAP (PHANTOM TAP)

Friday from 10:00 – 11:50 in Sunset 2 at Planet Hollywood

Audience: Red Teams, it could also be used by Blue Teams.

### Diana Dragusin & Etienne Champetier

PhanTap (phantom tap) is an 'invisible' network tap aimed at red teams. With limited physical access to a target building, this tap can be installed inline between a network device and the corporate network. PhanTap is silent in the network and does not affect the victim's traffic, even in networks having NAC (Network Access Control 802.1X - 2004). PhanTap will analyze traffic on the network and mask its traffic as the victim device. It will mount a tunnel back to a remote server, giving the attacker a foothold in the network for further exploitation and pivoting. The physical device for PhanTap is currently a small, inexpensive and disposable router running OpenWrt, we've been testing the GL.iNet GL-AR150. Moreover, PhanTap is fully based on Linux packages and can be ported to any Linux distribution.

# DEMO LABS

## PHISHING SIMULATION

Friday from 12:00 – 13:50 in Sunset 5 at Planet Hollywood

Audience: Defense

**Jyoti Raval**

Phishing Simulation tool mainly aims to increase phishing awareness & understanding by providing an intuitive tutorial and customized assessment to assess people's action on any given situation without performing actual phishing activity; and further gives analysis of what is the current awareness posture of targeted users.

The tool has below modules:

- Tutorial -> To increase the awareness by providing an interactive and intuitive tutorial
- Assessment -> To evaluate the current understanding and actions of user on any given situation
- Setup Test -> This module let's any user to create the customized campaign and target multiple users at same time
- Analysis -> Graphical representation to understand the current awareness posture

<https://github.com/jenyraval/Phishing-Simulation>

## PIVOTSUITE: HACK THE HIDDEN NETWORK - A NETWORK PIVOTING TOOLKIT

Saturday from 14:00 – 15:50 in Sunset 3 at Planet Hollywood

Audience: Offense (Red Teamers / Penetration Testers)

**Manish Gupta**

PivotSuite is a portable, platform independent and powerful network pivoting toolkit, Which helps Red Teamers / Penetration Testers to use a compromised system to move around inside a network. It is a Standalone Utility, Which can use as a Server or as a Client. PivotSuite as a Server : If the compromised host is directly accessible (Forward Connection) from Our pentest machine, Then we can run pivotsuite as a server on compromised machine and access the different subnet hosts from our pentest machine, Which was only accessible from compromised machine. PivotSuite as a Client : If the compromised host is behind a Firewall / NAT and isn't directly accessible from our pentest machine, Then we can run pivotsuite as a server on pentest machine and pivotsuite as a client on compromised machine for creating a reverse tunnel (Reverse Connection). Using this we can reach different subnet hosts from our pentest machine, which was only accessible from compromised machine.

<https://github.com/RedTeamOperations/PivotSuite>

## QILING

Sunday from 10:00 – 11:50 in Sunset 6 at Planet Hollywood

Audience: Reverse Engineers, Hardware (IoT) Hackers

**KaiJern, Lau & Dr. Nguyen Anh Quynh**

QiLing, a cross platform and multi architecture binary emulator, it will also able to do the following:

To execute binary applications for (Windows, Mac, Linux, Android, iOS, etc) and CPU architectures (Intel, Arm, AArch64 and Mips).

To be executed multiple platforms: Windows, MacOS, Linux, BSD. Sandbox analysis, so potential malicious activities are under control.

Provide Python instrumentation framework, so users can build add-on plugins to customize runtime analysis.

Analyze & report the code execution in friendly and fully customizable high-level format.

Besides working as an independent tool, QiLing also provides plugins for disassemblers such as Ghidra & IDA Pro. QiLing is designed to be lightweight and pluginable emulator. To handle real binaries reasonably, it should be fast, and offer instrumentation capability for users to build customized analysis.

- Able to handle hardware emulation

- Dynamically patch binary during execution in order to redirecting execution flow to bypass non critical check.

- Handle full binary emulation, not just raw code without context. To achieve this, emulate some parts of OS (such as syscalls, system libraries and part of kernel).

- Enable user-customized analysis via a Python framework.

QiLing is a opensource project.

## REVERSE ENGINEERING EMBEDDED ARM WITH GHIDRA

Friday from 10:00 – 11:50 in Sunset 4 at Planet Hollywood

Audience: Offense, Defense, AppSec, Mobile, Hardware

**Max Compston**

The ARM processor is the most prevalent processor in the world. ARM devices encompass mobile phones, network devices and appliances, and devices comprising what is now called the Internet of Things. Before April 2019, the only professional tool available for Reverse Engineering ARM processors was IDA Pro. With the release of Ghidra by the National Security Agency (NSA) to the Open Source Community this April, a professional grade Reverse Engineering tool is now available for ARM. This Demo Lab setup will include a Linux Host Laptop running Ubuntu Linux. The target system is an embedded Raspberry Pi ARM v8a running Ubuntu Linux Core. This demonstration will consist of static Reverse Engineering a demonstration Banking Application daemon using Ghidra. Static analysis of the fictitious application with this tool should reveal areas prone to PLT/GOT infection. This analysis will focus on shared libraries prone to infection. Next, an Injection / Hook program will perform Linux PTRACE Injection / Function Hooking on the Banking Application. The function hooking is based upon the results from the Ghidra analysis performed earlier. The hook function will send the user data back to our host using a method unknown to the developer of the Banking Application.



## RHODIOLA

Sunday from 10:00 – 11:50 in Sunset 5 at Planet Hollywood

Audience: Offense

### Utku Sen

Adversaries need to have a wordlist or combination-generation tool while conducting password guessing attacks. To narrow the combination pool, researchers developed a method named “mask attack” where the attacker needs to assume a password’s structure. Even if it narrows the combination pool significantly, it’s still too large to use for online attacks or offline attacks with low hardware resources. In the real world, a password’s structure is an unknown value, just like the password itself. Even if we specify a password structure with masks, we are still brute forcing characters in the mask. When we analyzed Ashley Madison and Myspace wordlists, we saw that they are mostly consists of sequential alpha characters. Which means that there is a high probability that they are meaningful words. Our research shows that 30% of the Ashley Madison wordlist and 36% of Myspace wordlist contains meaningful English words. Rhodiola tool is developed to narrow the combination pool by creating a personalized wordlist for target people. It finds interest areas of a given user by analyzing his/her tweets, and builds a personalized wordlist. Wordlist consists of most used nouns & proper nouns, paired nouns & proper nouns, cities and years related to detected proper nouns.

## SHADOW WORKERS: BACKDOORING WITH SERVICE WORKERS

Saturday from 14:00 – 15:50 in Sunset 6 at Planet Hollywood

Audience: Offensive Security, AppSec

### Emmanuel Law & Claudio Contin

This presentation is focused around Shadow Workers, a tool that came out of our research on service workers. Service Workers are a new addition to modern browser and often used to extend offline capabilities to a website. With this tool, we weaponized service workers to include the ability to implant a pseudo backdoor in the browser and ghost through a victim’s browser session to sniff, manipulate, and even proxy data silently. We’ll demo the various persistence mechanisms our tool provides to keep service workers alive and demo how MITM can be done at the browser layer.

<https://github.com/shadow-workers/shadow-workers>

## SHELLCODE COMPILER

Saturday from 14:00 – 15:50 in Sunset 5 at Planet Hollywood

Audience: Anyone interested in shellcode development

### Ionut Popescu

Shellcode Compiler is a program that compiles C/C++ style code into a small, position-independent and NULL-free shellcode for Windows and Linux. It is possible to call any Windows API function or Linux syscall in a user-friendly way. The tool allows users to write custom shellcodes by providing an easy way to call functions or system calls. It does not have

all the capabilities of a compiler, but it simplifies a lot the shellcode development process. There is no need to write assembler, it is only required to declare and call functions or system calls. Under the hood there is, of course, a custom compiler which compiles C/C++ style code into ASM which is later assembled using Keystone framework. Before the tool presentation, we will go into a deep dive on the shellcode development process for both Windows and Linux (32 bits only to keep it short and simple).

<https://github.com/NyTROST/ShellcodeCompiler>

## SILENTRINITY

Saturday from 14:00 – 15:50 in Sunset 4 at Planet Hollywood

Audience: Offense

### Marcello Salvati

SILENTRINITY is an asynchronous post-exploitation agent powered by Python, IronPython, C# and .NET’s DLR (Dynamic Language Runtime), it attempts to weaponize and demonstrate the flexibility that BYOI (Bring Your Own Interpreter) payloads have over traditional C# implants. What are BYOI payloads? Turns out by harnessing the sheer craziness of the .NET framework, you can embed entire interpreters inside of .NET languages allowing you to natively execute scripts written in third-party languages (like Python) on windows! Not only does this allow you to dynamically access all of the .NET API from a scripting language of your choosing, but it also allows you to still remain completely in memory and has a number of advantages over traditional C# payloads! Essentially, BYOI payloads allow you to have all the “power” of PowerShell, without going through PowerShell in anyway! Additionally, you can nest multiple interpreters within each other to perform what I’ve coined “engine inception”! If you’re interested in bleeding-edge and out of the ordinary C#/.NET offensive trade-craft, this is the demo for you!

<https://github.com/byt3bl33d3r/SILENTRINITY>

## SOFRIDA - DYNAMIC ANALYSIS TOOL FOR MOBILE APPS WITH CLOUD BACKEND

Friday from 10:00 – 11:50 in Sunset 6 at Planet Hollywood

Audience: Offense: Mobile Application Pentesters, Hackers Defense: Cloud Backend Operators Mobile Application Developers who use cloud SDK

### Hyunjun Park & Soyeon Kim

Mobile app developers are increasingly using cloud services to implement features such as storage, push notifications, and user data analysis. Popular cloud service including AWS provides SDK and credential keys that allow mobile apps to authenticate and authorize cloud resources so that developers can implement features by calling APIs. However, we identify a vulnerability that those credential keys can be obtained by attackers. Within this demo, we will present how to steal cloud credential keys with soFrida: a dynamic analysis tool, powered by Frida. With soFrida, security researchers or engineers can quickly collect Android APKs and analyze cloud vulnerabilities in Android apps, helping to prevent

# DEMO LABS

serious security incidents such as data leaks. We have discovered 2,700 potentially vulnerable mobile apps by using sofrida and currently collaborate with the cloud service provider to eliminate security vulnerabilities. Detailed statistics can be found on our website: <https://sofrida.github.io>

<https://sofrida.github.io>

## SPARTACUS AS A SERVICE (SAAS)

Friday from 12:00 – 13:50 in Sunset 3 at Planet Hollywood

Audience: Offense for the end user

Mike Kiser

The Third Servile War was over. The slave army has been defeated, and the survivors are offered a pardon by their Roman captors. The only requirement was that they identify Spartacus, their leader (Kirk Douglas). Rather than give away his identity, however, they all begin to yell out "I'm Spartacus!"—thus preserving his anonymity by overwhelming the Romans with possibilities. (Spoiler alert: they all die as a result.) "Spartacus as a Service (SaaS)" is an open-source proof-of-concept is introduced that facilitates these obfuscation techniques. This will allow for automatic obfuscation of a chosen identity on a small scale, and lessons learned from its usage will be discussed. Current version at: <https://github.com/derrumbe/Spartacus-as-a-Service> Open-source tool written largely in Node.js under an MIT license OAuth is used for authentication and authorization Content is generated via a Markov chain using sources such as Jane Austen, political platforms, and Aaron Franklin's book on BBQ Amazon Mechanical Turk may be used to circumvent captchas Note that this is not a tool that \*prevents\* targeted advertising — instead it seeks to dilute the value of information that companies know about a user. It obfuscates the real content so that outsiders cannot tell what the real content (or in some cases, who the person) actually is.

<https://github.com/derrumbe/Spartacus-as-a-Service>

## SRUJAN: SAFER NETWORKS FOR SMART HOMES

Saturday from 10:00 – 11:50 in Sunset 4 at Planet Hollywood

Audience: Defense, Network, Hardware, IOT Security

Sanket Karpe & Parmanand Mishra

Srujan is a new type of network segregation system, based on Raspberry Pi, that can be easily deployed on home networks. It allows home users to segregate the devices connecting to their home networks based on the threat profile. User can keep their smart home devices separate from their computers and mobile devices to mitigate risk of cross infection from low-trust devices like smart cameras, speakers and thermostats. Srujan was created to address the challenges around the plethora of IOT devices being deployed in smart homes that are vulnerable and do not receive patches. Srujan can intelligently segregate the home network into different zones based on the device type. It automatically identifies and alerts users when the IOT devices attempt to contact any IP or domain which

has been blacklisted by Google Safe Browsing.

Srujan provides the following features:

- Intelligent segregation of devices based on their type
- Ability to create network usage stats for each device
- Ability to quarantine untrusted devices
- Easy to integrate with SIEM
- Ability to lookup IP/Domain against Google Safe Browsing.
- Integration with ANWI (All New Wireless IDS)
- Prevent call-home pings to manufacturer for enhanced privacy.

## TAINTEDLOVE

Friday from 12:00 – 13:50 in Sunset 6 at Planet Hollywood

Audience: AppSec

Benoit Côté-Jodoin

TaintedLove is a dynamic security analysis tool for Ruby. It leverages Ruby's object tainting and monkey patching features to identify potentially vulnerable code paths at runtime. TaintedLove is library agnostic and provides a simple framework to extend the detection of unsafe method usage and user input tracking.

[https://github.com/shopify/tainted\\_love](https://github.com/shopify/tainted_love)

## USB-BOOTKIT — NEW BOOKIT VIA USB INTERFACE IN SUPPLY CHAIN ATTACKS

Sunday from 10:00 – 11:50 in Sunset 4 at Planet Hollywood

Audience: Offense, Defense and Hardware.

Haowen Bai

USB-Bootkit, a new type of Bootkit via the USB interface, contains malicious code inside the USB device that gets executed every time the system boots up. The malicious device, located either on the motherboard or inside external HID devices such as the keyboard, is invisible to ordinary users and capable to re-infect the system after the OS getting reinstalled, the hard drive being formatted or even replaced.

In order to make it looks innocuous, we implanted the USB-Bootkit inside a keyboard without changing the outward appearance. Supply chain attacks could be leveraged to replace the device and modify boot sequences accordingly. Once it is used by the target, we are able to carry out attacks persistently. Legacy and UEFI mode are covered in one USB to adapt the target system automatically. In the demonstration, the attack originates from the malicious keyboard and is able to compromise the full patched Windows 10 x64 operating system since power-on. The USB-Bootkit will get disconnected automatically afterwards to avoid being discovered when the victim logs into the operating system.

<https://github.com/RedDrip7/USB-Bootkit>



## VULMAP: ONLINE LOCAL VULNERABILITY SCANNERS PROJECT

Sunday from 10:00 – 11:50 in Sunset 3 at Planet Hollywood  
Audience: Offense, Defense

### Yavuz Atlas & Fatih Ozel

Vulmap is an open source online local vulnerability scanner project. It consists of online local vulnerability scanning scripts for Windows and Linux. These scripts can be used for defensive and offensive purposes. It is possible to conduct vulnerability assessments by using these scripts. Also they can be used for privilege escalation by pentesters/red teamers. Vulmap scans vulnerabilities on localhost, shows related exploits and downloads them. It basically, scan localhost to gather installed software information and ask Vulmon API if there are any vulnerabilities and exploits related with installed software. If any vulnerability exists, Vulmap shows CVE ID, risk score, vulnerability's detail link, exploit ids and exploit titles. Exploits can be downloaded with Vulmap also. Main idea of Vulmap is getting real-time vulnerability data from Vulmon instead of relying of a local vulnerability database. Even the most recent vulnerabilities can be detected with this approach. Also its exploit download feature helps privilege escalation process. Since most Linux installations have Python, Vulmap Linux is developed with Python while Vulmap Windows is developed with PowerShell to make it easy to run it on most Windows versions without any installation.

<https://github.com/vulmon/Vulmap>

## WIFI KRAKEN — SCALABLE WIRELESS MONITORING

Saturday from 10:00 – 11:50 in Sunset 1 at Planet Hollywood  
Audience: Offense, Defense, Hardware

### Mike Spicer

This tool is the culmination of lessoned learned during the last 3 years of wireless monitoring at DEF CON using tools like the #WiFiCactus. This demo will show you the software and hardware needed to build a robust wireless monitoring sensor network that is capable of capturing everything up to 802.11ac including Bluetooth. This demo will include a distributed capture network that will take captured data from multiple nodes and send it back to a single capture server. This project will show you how to use advanced features of Kismet Wireless to increase the amount of data you capture. Wireless threats and attacker tactics will be discussed and identified as they happen in the environment. Data analytic techniques will be demonstrated and discussed using tools like Wireshark, NetworkMiner and PCAPinator.

<http://palshack.org/def-con-27-demolab/>

## ZIGBEE HACKING: SMARTER HOME INVASION WITH ZIGDIGGITY

Sunday from 10:00 – 11:50 in Sunset 2 at Planet Hollywood  
Audience: Offense, Hardware, Product, IoT, Zigbee, Zigbee Hacking

### Francis Brown & Matt Gleason

Do you feel safe in your home with the security system armed? You may reconsider after watching a demo of our new hacking toolkit, ZigDiggity, where we target door & window sensors using an "ACK Attack". ZigDiggity will emerge as the weapon of choice for testing Zigbee-enabled systems, replacing all previous efforts. Zigbee continues to grow in popularity as a method for providing simple wireless communication between devices (i.e. low power/traffic, short distance), & can be found in a variety of consumer products that range from smart home automation to healthcare. Unfortunately, existing Zigbee hacking solutions have fallen into disrepair, having barely been maintained, let alone improved upon. Left without a practical way to evaluate the security of Zigbee networks, we've created ZigDiggity, a new open-source pentest arsenal from Bishop Fox. Updates include migration to better hardware for testing (e.g. SDRs), and a slew of newly implemented Zigbee attacks types. Our DEMO-rich presentation showcases ZigDiggity's attack capabilities by pitting it against common Internet of Things (IoT) products that use Zigbee. Come experience the future of Zigbee hacking, in a talk that the New York Times will be hailing as "a veritable triumph of the human spirit." ... ya know, probably

<https://github.com/BishopFox/zigdiggity>

# VENDORS

## ATTIFY STORE

 **ihackiot.com**

### ATTIFY

<https://www.attify-store.com/>

Attify provides educational learning kits for security enthusiasts to acquire skillsets in various IoT areas such as Embedded and Hardware Device Hacking, Radio Exploitation, BLE, ZigBee Analysis and more. Our learning kits are suited both for experienced professionals as well as beginners who are about to kickstart their security

### BAIDU

<https://www.baidu.com/>

## CALYX



### CALYX INSTITUTE

<https://www.calyxinstitute.org/>

The Calyx Institute is a member-supported non-profit privacy organization. We host Tor exit nodes, have a free VPN service and are developing a privacy and security focused Mobile phone operating system, CalyxOS. Become a member and you could get great free membership premiums such as a mobile hotspot with unlimited unthrottled & uncapped mobile data for a year, or a Google Pixel 2 phone with CalyxOS pre-installed on it. The Calyx Institute is a member-supported non-profit privacy organization. We host Tor exit nodes, have a free VPN service and are developing a privacy and security focused Mobile phone operating system, CalyxOS. Become a member and you could get great free membership premiums such as a mobile hotspot with unlimited unthrottled & uncapped mobile data for a year, or a Google Pixel 2 phone with CalyxOS pre-installed on it. The Calyx Institute is a member-supported non-profit privacy organization. We host Tor exit nodes, have a free VPN service and are developing a privacy and security focused Mobile phone operating system, CalyxOS. Become a member and you could get great free membership premiums such as a mobile hotspot with unlimited unthrottled & uncapped mobile data for a year, or a Google Pixel 2 phone with CalyxOS pre-installed on it.



**CAPITOL**  
Technology University

### CAPITOL TECHNOLOGY UNIVERSITY

<http://www.captechu.edu/>

Capitol Technology University's mission is to educate individuals for professional opportunities. A STEM focused institution of higher education, providing undergraduate and graduate degrees in engineering, information sciences, and technology leadership, that has flexibility and opportunities to grow, and that adapts offerings to emerging workforce needs.



### EFF

<https://eff.org/join>

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We guard free speech online, fight illegal surveillance, support emerging technologies, defend digital innovators, and work to ensure that our rights and freedoms are enhanced, rather than eroded, as our use of technology grows.



### GHETTO GEEKS

After many years in the shadows, we're back and better than ever. If you have ever seen what we create, you know we bring a delightful poke at many subjects we enjoy. From Math to computers and beyond we keep making the magic sauce for your clothing needs. Come on by and take a look and you won't be disappointed, you may even find a chuckle while checking things out.



---

## GUNNAR OPTICS

<https://gunnar.com/>

GUNNAR is the only patented computer eyewear recommended by doctors to protect and enhance your vision. GUNNAR's premium computer eyewear defends eyes against short and long-term effects of digital eyestrain due to exposure to digital screens and artificial blue light. GUNNAR's patented lens technology is specifically formulated to combat the harmful effects of digital eye strain to protect both your eye and body health. The result - improved clarity, focus and performance. GUNNAR is the only patented computer eyewear recommended by doctors to protect and enhance your vision. GUNNAR's premium computer eyewear defends eyes against short and long-term effects of digital eyestrain due to exposure to digital screens and artificial blue light. GUNNAR's patented lens technology is specifically formulated to combat the harmful effects of digital eye strain to protect both your eye and body health. The result - improved clarity, focus and performance. GUNNAR is the only patented computer eyewear recommended by doctors to protect and enhance your vision. GUNNAR's premium computer eyewear defends eyes against short and long-term effects of digital eyestrain due to exposure to digital screens and artificial blue light. GUNNAR's patented lens technology is specifically formulated to combat the harmful effects of digital eye strain to protect both your eye and body health. The result - improved clarity, focus and performance.

**GUNNAR**  
COMPUTER EYEWEAR

---

## HACKER BOXES

<http://www.hackerboxes.com/>

Hacker Boxes is the monthly subscription box service for hardware hacking, DIY electronics, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. HackerBox Hackers connect online as a community of experience, support, and ideas. It's like having a tiny hacker con in your mailbox every month!



---

## HACKER PUZZLE ADVENTURE CUBE

This DEF CON, We're excited to launch a community-driven fundraiser to build the Hacker Puzzle Adventure Cube, an interactive art project celebrating the magic and wizardry of hacking. With your support, this ~3 foot square electronic puzzle box will contain a series of challenges ranging from classic CTF-style to lockpicking, crypto, RF, reverse engineering, and audiovisual, delivered in a sleek and visually stunning package. The finished cube will be showcased at hacker cons and events, engaging community collaboration as participants solve the ultimate hacker challenge. Stop by our booth to learn more!



---

## HACKER WAREHOUSE

<https://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 the HackerWarehouse.com.



---

## HAK5 LLC

<https://shop.hak5.org/>

Discover the devices that have found their way into the hearts and tool-kits of the modern hacker. Notable for ease of use. Celebrated by geek culture. From comprehensive WiFi audits to covert network implants and physical access mayhem - Hak5 Gear gets the job done. Check out the brand new 2019 gear from Hak5 complimenting an arsenal of WiFi Pineapples and USB Rubber Duckies!



# VENDORS

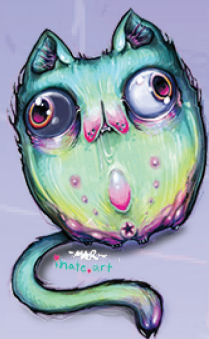


---

## KEYPORT, INC.

<https://www.mykeyport.com/>

Keyport® combines keys, pocket tools, & smart tech into one everyday multi-tool. We will be selling our latest modular product line (DEF CON 27 Editions) including the Keyport Slide 3.0 & Keyport Pivot (holds your existing keys), Anywhere Tools™ Modules, and the debut of OmniFob™. If you want a Keyport Slide made on site, don't forget to bring your keys to the vendor area!



---

## MAR

<http://ihate.art>

For the past decade, DEF CON resident artist Mar Williams's artwork has been a part of the DEF CON experience. For DEF CON 27, Mar will be doing a live, onsite mural painting. Once the mural is completed, it will be broken into individual pieces and auctioned off, with half the proceeds going to support the Electronic Frontier Foundation. Mar will also be selling original artwork as well as limited-run art prints and other arty, vaguely-cat-shaped baubles. IG @spuxo



---

## NETOOL LLC

<https://netool.io/>

Netool.io - A pocket sized network analyzer. Discovery patch detection, packet sniffing to pcap file, tagged VLAN detection and much more. Make network diagnostics and penetration testing easy.



**no starch  
press**

---

## NO STARCH PRESS

<https://nostarch.com/>

No Starch Press publishes the finest in geek entertainment — bestsellers like Python Crash Course, Linux Basics for Hackers, Hacking: The Art of Exploitation, and The Game Console. We focus on programming, security, hacking, and alternative operating systems. Our titles have personality and attitude, our authors are passionate about their subjects, and we read and edit every book that we publish. Readers appreciate our straightforward presentation, fearless approach to the complex world of technology, and desire to give back to the hacking community.



---

## NUAND LLC

<https://nuand.com/bladeRF>, <https://nuand.com/shop/>

Nuand provides low-cost, USB 3.0 SDRs (Software Defined Radio) for enthusiasts, and experts alike. Come checkout the brand new bladeRF micro in action! Stop by our table to see our demos and find out more about bladeRF, GNURadio, and Software Defined Radios!



---

## OWASP

<https://www.owasp.org/>

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies, and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.



---

## RAPID7

<http://www.rapid7.com/>

Rapid7 is advancing security to accelerate innovation. Learn how our Insight cloud delivers shared visibility, analytics, and automation at [www.rapid7.com](http://www.rapid7.com).



---

## SCAM STUFF

<https://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!

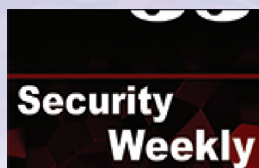


---

## SECURITY WEEKLY

<https://securityweekly.com/>

Security Weekly is the security podcast network for the security community, distributing free podcasts and media since 2005. We connect the security industry and the security community through our security market validation programs. We view our relationships with the security industry as partnerships, not sponsorships. Security Weekly works closely with each partner to help them achieve their marketing goals and gain traction in the security market.



---

## SHADOWVEX

<http://store.shadowvexindustries.com/>

Shadowvex Industries and Miss Jackalope have mysteriously appeared from the digital underground for over 20 years! Purveyors of hacker-relevant limited edition Clothing, DJ mixes, Stickers, Buttons, Patches, Unique Art and 0-day swag specifically for DEF CON 27! If you want to bring home your piece of DEF CON history you need to get here early... so follow the music in the vending area to find our booth!



---

## SIMPLE WIFI

<https://www.simplewifi.com/>

Simple WiFi designs & manufactures in the U.S.A., high quality WiFi antennas for wireless networking.



---

## SPARROWS

<http://www.sparrowslockpicks.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 LOCK PICKS, Entry Tools, PRACTICE LOCKS, Bypass tools, Urban Escape & Evasion hardware and items that until recently were sales restricted. We will be displaying a full range of gear including our newly released DIMPLE PICKS, Revolver and Ranger. The Night Crawler set 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.



# VENDORS



## TENCENT

<https://www.tencent.com/zh-cn/index.html>

Tencent is an internet-based technology and cultural enterprise headquartered in Shenzhen, China. Founded in 1998, Tencent's mission is to "improve the quality of life through Internet value-added services". Tencent Security Response Center is responsible for the antihacking, monitoring and analyzing security threats of Tencent. We are protecting over 1,000,000,000 netizens around the world and are building an open platform for technology sharing for a better cyber security ecosystem.



## THE TOR PROJECT

<https://www.torproject.org/>

The Tor Project is a nonprofit that develops free and open source software to protect people from tracking, censorship, and surveillance online. Stop by our table to learn more, pick up some gear, and find out how you can get involved. The Tor Project is a nonprofit that develops free and open source software to protect people from tracking, censorship, and surveillance online. Stop by our table to learn more, pick up some gear, and find out how you can get involved.



## T000L

<https://toool.us/equipment.html>

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.



## TSOK

<https://www.defcononline.com/>

Recorded sessions from DEF CON 27 (including the 4 tracks and some villages) available for purchase on a USB or access to online streaming for affordable prices. Streaming content available within 10 business days post event. See our two on site sales stations at Paris Bally's to purchase or visit [www.defcononline.com](http://www.defcononline.com)



## U.N.I.C.O.R.N.

N/A

The union of Unicorns in China's Internet security ecology, this time not just include UnicornTeam, come here to pick up awesome offensive and defensive hacker tools from our vendor!



## UNIVERSITY OF ADVANCING TECHNOLOGY

<https://www.uat.edu/>

UAT is an elite intimate private college in Tempe, AZ focused on educating students in advancing technology who desire to innovate in the areas of emerging technology disciplines including Advancing Computer Science, Information Security, Game and New Media technologies.



## 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/>.



# CONNECT

## OFFICIAL SITES

WEBSITE: [HTTPS://DEFCON.ORG](https://defcon.org)

DEF CON MEDIA: [HTTPS://MEDIA.DEFCON.ORG](https://media.defcon.org)

DEF CON GROUPS: [HTTPS://DEFCONGROUPS.ORG](https://defcongroups.org)

DEF CON FORUMS: [HTTPS://FORUM.DEFCON.ORG](https://forum.defcon.org)

## U.S. SOCIAL MEDIA



TWITTER: [HTTPS://TWITTER.COM/DEFCON](https://twitter.com/DEFCON)



FACEBOOK: [HTTPS://FACEBOOK.COM/DEFCON/](https://facebook.com/DEFCON/)



INSTAGRAM: [HTTPS://WWW.INSTAGRAM.COM/WEAREDEFCON/](https://www.instagram.com/wearedefcon/)



REDDIT: [HTTP://WWW.REDDIT.COM/R/DEFCON](http://www.reddit.com/r/DEFCON)



DOWNLOAD THE PRESENTATION MATERIALS  
AND MORE FROM THE DEF CON MEDIA SERVER  
AT:

[HTTPS://MEDIA.DEFCON.ORG/DEF CON 27/](https://media.defcon.org/DEFCON27/)

# FIRESIDES LOUNGE

## FRIDAY

### DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

Friday at 20:00 in Sin City Theatre at Planet Hollywood  
Christian “quaddi” Dameff, Jeff “r3plicant” Tully MD, Suzanne Schwartz MD, Marie Moe PhD, Billy Rios, Jay Radcliffe

### PANEL: DEF CON GROUPS

Friday at 22:15 in Sin City Theatre at Planet Hollywood  
Brent White / B1TK1LL3R, Jayson E. Street, Darington, April Wright, Tim Roberts (byt3boy), Casey Bourbonnais, sOups

## SATURDAY

### MEET THE EFF - MEETUP PANEL

Saturday at 20:00 in Sin City Theatre at Planet Hollywood  
Kurt Opsahl, Camille Fischer, Bennett Cyphers, Nathan ‘nash’ Sheard, Shahid Buttar

### WE HACKED TWITTER! AND THE WORLD LOST THEIR SH\*T OVER IT!

Saturday at 22:15 in Sin City Theatre at Planet Hollywood  
Mike Godfrey, Matthew Carr

# -THURSDAY-

DC 101 IN TRACK 4	
10:00	Exploiting Windows Exploit Mitigation for ROP Exploits Omer Yair
11:00	Breaking Google Home: Exploit It with SQLite (Magellan) Wenxiang Qian, YuXiang Li, HuiYu Wu
12:00	Are Quantum Computers Really A Threat To Cryptography? A Practical Overview Of Current State-Of-The-Art Techniques With Some Interesting Surprises Andreas Baumhof
13:00	Intro to Embedded Hacking -- How you too can find a decade old bug in widely deployed devices. [REDACTED] Deskhphones, a case study. Philippe Lauheret
14:00	Web2Own: Attacking Desktop Apps From Web Security's Perspective Junyu Zhou, Ce Qin, Jianing Wang
15:00	DEF CON 101 Panel Highwiz, Nikita, Will, n00bz, Shaggy, SecBarbie, Tottenkoph
15:30	

## 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 27 CONTESTS AT OUR CONTESTS CLOSING CEREMONIES, FROM 14:00 - 15:30PM IN TRACK 4!

BLACK BADGE WINNERS WILL BE ANNOUNCED DURING THE MAIN CLOSING CEREMONIES AT 16:00.



	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	<p>Behind the Scenes of the DEF CON 27 Badge</p> <p>Joe Grand (Kingpin)</p>	<p>Hacking Congress: The Enemy Of My Enemy Is My Friend</p> <p>Former Rep. Jane Harman, Rep. James Langevin, Jen Ellis, Cris Thomas, Rep. Ted Lieu</p>	<p>Behind the Scenes: The Industry of Social Media Manipulation Driven by Malware</p> <p>Olivier Bilodeau, Masarah Paquet-Clouston</p>	<p>Duplicating Restricted Mechanical Keys</p> <p>Bill Graydon, Robert Graydon</p>
11:00	<p>Don't Red-Team AI Like a Chump</p> <p>Ariel Herbert-Voss</p>	<p>The Tor Censorship Arms Race: The Next Chapter</p> <p>Roger Dingledine</p>	<p>All the 4G Modules Could Be Hacked</p> <p>XiaoHuiHui, Ye Zhang, ZhengHuang</p>	<p>Evil eBPF In-Depth: Practical Abuses of an In-Kernel Bytecode Runtime</p> <p>Jeff Dileo</p>
12:00	<p>Process Injection Techniques - Gotta Catch Them All</p> <p>Itzik Kotler, Amit Klein</p>	<p>Phreaking Elevators</p> <p>WillC</p>	<p>Infiltrating Corporate Intranet Like NSA _Pre-auth RCE on Leading SSL VPNs</p> <p>Orange Tsai, Meh Chang</p>	<p>API-Induced SSRF: How Apple Pay Scattered Vulnerabilities Across the Web</p> <p>Joshua Maddux</p>
13:00	<p>HackPac: Hacking Pointer Authentication in iOS User Space</p> <p>Xiaolong Bai, Min (Spark) Zheng</p>	<p>HVACking: Understand the Difference Between Security and Reality!</p> <p>Douglas McKee, Mark Bereza</p>	<p>No Mas—How One Side-Channel Flaw Opens ATM, Pharmacies and Government Secrets Up to Attack</p> <p>phar</p>	<p>More Keys Than A Piano: Finding Secrets In Publicly Exposed Ebs Volumes</p> <p>xBen “benmap” Morris</p>
14:00	<p>Harnessing Weapons of Mac Destruction</p> <p>Patrick Wardle</p>	<p>Are Your Child's Records at Risk? The Current State of School Infosec</p> <p>Bill Demirkapi</p>	<p>How Deep Learning Is Revolutionizing Side-Channel Cryptanalysis</p> <p>Elie Bursztein, Jean Michel Picod</p>	<p>Practical Key Search Attacks Against Modern Symmetric Ciphers</p> <p>Daniel “ufurnace” Crowley, Daniel Pagan</p>
15:00	<p>MOSE: Using Configuration Management for Evil</p> <p>Jayson Grace</p>	<p>Change the World, cDc Style: Cow tips from the first 35 years</p> <p>Joseph Menn, Peiter Mudge, Zlatko, Chris Dildog Rioux, Deth Vegetable, Omega</p>	<p>100 Seconds of Solitude: Defeating Cisco Trust Anchor With FPGA Bitstream Shenanigans</p> <p>Jatin Kataria, Rick Housley, Ang Cui</p>	<p>Relaying Credentials Has Never Been Easier: How to Easily Bypass the Latest NTLM Relay Mitigations</p> <p>Marina Simakov, Yaron Zinar</p>
16:00	<p>Please Inject Me, a x64 Code Injection</p> <p>Alon Weinberg</p>	<p>I Know What You Did Last Summer: 3 Years of Wireless Monitoring at DEF CON</p> <p>d4rkm4tter (Mike Spicer)</p>	<p>Surveillance Detection Scout - Your Lookout on Autopilot</p> <p>Truman Kain</p>	<p>The JOP ROCKET: A Supremely Wicked Tool for JOP Gadget Discovery, or What to Do If ROP Is Too Easy</p> <p>Dr. Bramwell Brizendine, Dr. Joshua Stroschien</p>
16:30	<p>Poking the S in SD cards</p> <p>Nicolas Oberli</p>	<p>Can You Track Me Now? Why The Phone Companies Are Such A Privacy Disaster</p> <p>U.S. Senator Ron Wyden</p>	<p>Breaking The Back End! It Is Not Always A Bug. Sometimes, It Is Just Bad Design!</p> <p>Gregory Pickett</p>	<p>Re: What's up Johnny?—Covert Content Attacks on Email End-to-End Encryption</p> <p>Jens Müller</p>

# -SATURDAY-

	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	Weaponizing Hypervisors to Fight and Beat Car and Medical Devices Attacks Ali Islam, Dan Regalado (DanuX)	Rise of the Hypebots: Scripting Streetwear finalphoenix	Information Security in the Public Interest Bruce Schneier	EDR Is Coming; Hide Yo Sh! Michael Leibowitz, Topher Timzen
11:00	Your Car is My Car Jmaxxx	HAKC THE POLICE Bill Swearingen	Hacking Your Thoughts - Batman Forever meets Black Mirror Katherine Pratt/GattaKat	Meticulously Modern Mobile Manipulations Leon Jacobs
12:00	How You Can Buy AT&T, T-Mobile, and Sprint Real-Time Location Data on the Black Market Joseph Cox	Defeating Bluetooth Low Energy 5 PRNG for Fun and Jamming Damien Cauquil (virtualabs)	Why You Should Fear Your "mundane" Office Equipment Daniel Romero, Mario Rivas	Zombie Ant Farm: Practical Tips for Playing Hide and Seek with Linux EDRs Dimitry Snezhkov
13:00	RACE - Minimal Rights and ACE for Active Directory Dominance Nikhil Mittal	GSM: We Can Hear Everyone Now! Campbell Murray, Eoin Buckley, James Kulikowski	Tag-side attacks against NFC Christopher Wade	SSO Wars: The Token Menace Alvaro Muñoz, Oleksandr Mirosh
14:00	SELECT code_execution FROM * USING SQLite; -- Gaining code execution using a malicious SQLite database Omer Gull	I'm on your phone, listening - Attacking VoIP Configuration Interfaces Stephan Huber, Philipp Roskosch	Zero bugs found? Hold my Beer AFL! How To Improve Coverage-Guided Fuzzing and Find New Odays in Tough Targets Maksim Shudrak	Next Generation Process Emulation with Binee Kyle Gwinnup, John Holowczak
15:00	Get Off the Kernel if You Can't Drive Jesse Michael, Mickey Shkatov	Reverse-Engineering 4g Hotspots for Fun, Bugs and Net Financial Loss g richter	State of DNS Rebinding - Attack & Prevention Techniques and the Singularity of Origin Gerald Doussot, Roger Meyer	.NET Malware Threats: Internals And Reversing Alexandre Borges
16:00	Reverse Engineering 17+ Cars in Less Than 10 Minutes Brent Stone	NOC NOC. Who's there? All. All who? All the things you wanted to know about the DEF CON NOC and we won't tell you about The DEF CON NOC	Confessions of an Nespresso Money Mule: Free Stuff & Triangulation Fraud Nina Kollars, Kitty Hegemon	Vacuum Cleaning SecurityöPinky and the Brain Edition jiska, clou (Fabian Ullrich)
16:30	Unpacking Pkgs: A Look Inside Macos Installer Packages And Common Security Flaws Andy Grant		Go NULL Yourself or: How I Learned to Start Worrying While Getting Fined for Other's Auto Infractions droogie	Apache Solr Injection Michael Stepankin



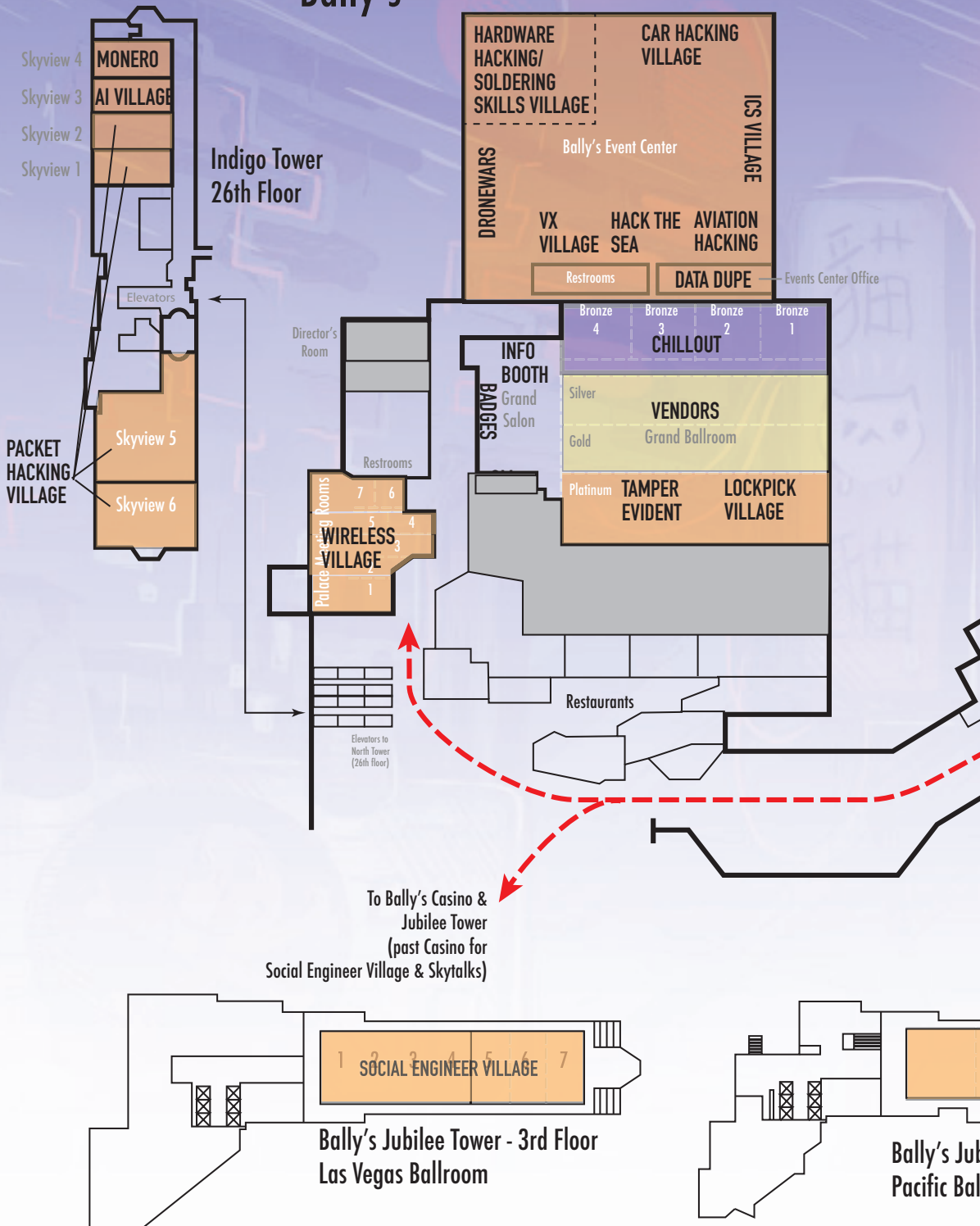
	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	Backdooring Hardware Devices By Injecting Malicious Payloads On Microcontrollers Sheila Ayelen Berta	Adventures In Smart Buttplug Penetration (testing) smea	Hacking WebAssembly Games with Binary Instrumentation Jack Baker	Your Secret Files Are Mine: Bug Finding And Exploit Techniques On File Transfer App Of All Top Android Vendors Xiangqian Zhang, Huiming Liu
11:00	The ABC of Next-Gen Shellcoding Hadrien Barral, Rémi Gérard-Stewart, Georges-Axel Jaloyan	SDR Against Smart TVs: URL and Channel Injection Attacks Pedro Cabrera Camara	Exploiting Qualcomm WLAN and Modem Over The Air Xiling Gong, Peter Pi	Say Cheese - How I Ransomware Your DSLR Camera Eyal Itkin
12:00	I'm In Your Cloud... Pwning Your Azure Environment Dirk-jan Mollema	Malproxying: Leave Your Malware at Home Hila Cohen, Amit Waisel	HTTP Desync Attacks: Smashing into the Cell Next Door albinowax	Help Me, Vulnerabilities. You're My Only Hope Jacob Baines
13:00	[ MI CASA-SU CASA ] My 192.168.1.1 is Your 192.168.1.1 Elliott Thompson	Sound Effects: Exploring Acoustic Cyber-weapons Matt Wixey	Owning The Clout Through Server-Side Request Forgery Ben Sadeghipour, Cody Brocius (Daeken)	Want Strong Isolation? Just Reset Your Processor Anish Athalye
14:00	Firmware Slap: Automating Discovery of Exploitable Vulnerabilities in Firmware Christopher Roberts	Cheating in eSports: How to Cheat at Virtual Cycling Using USB Hacks Brad Dixon	The Ether Wars: Exploits, counter-exploits and honeypots on Ethereum Bernhard Mueller, Daniel Luca	Contests Awards Ceremony Contests & Events
15:00	Closed			
16:00	Closing Ceremonies The Dark Tangent & Goons			

InfoCon  
Hacking Conference Archive  
[www.infocon.org](http://www.infocon.org)

# DAYTIME MAP

DEF CON 27 PART

Bally's





# PARIS & BALLY'S

## PARIS & BALLY'S FLOORPLAN



# DAYTIME MAPS

## DEF CON 27 FLAMINGO FLOORPLAN

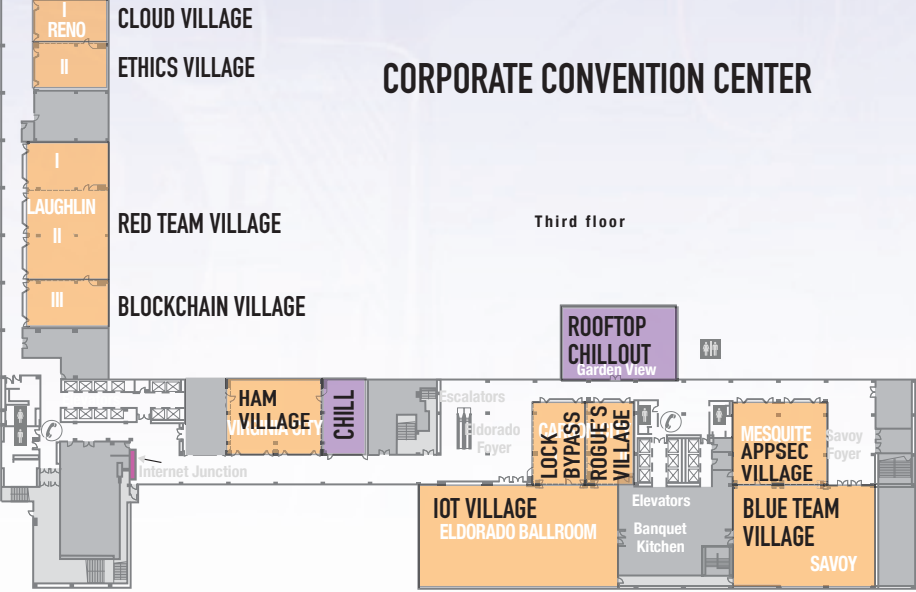
### EXECUTIVE CONFERENCE CENTER

#### LOWER LEVEL



### CORPORATE CONVENTION CENTER

Third floor





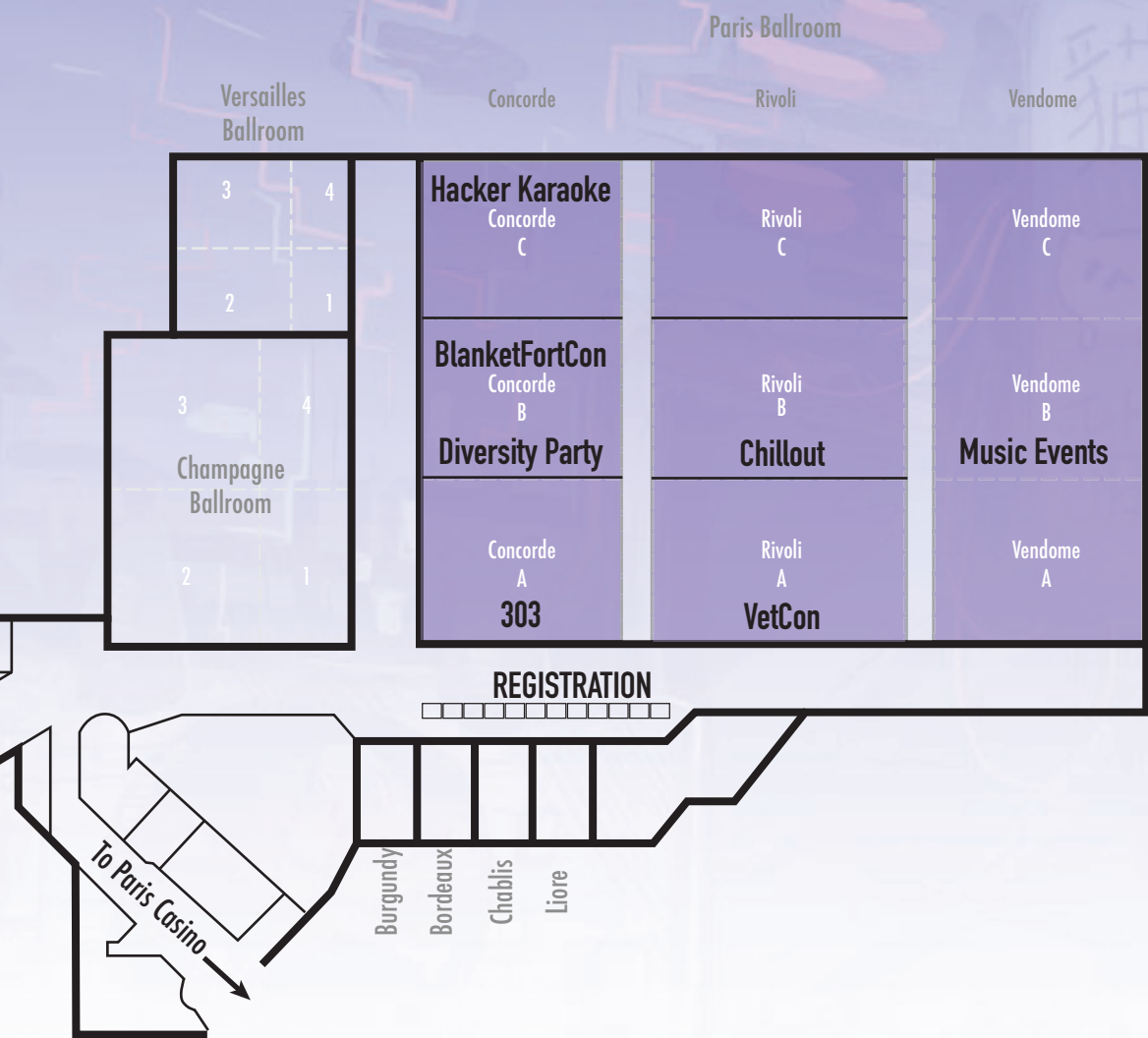
# FLAMINGO & PLANET HOLLYWOOD

## DEF CON 27 PLANET HOLLYWOOD FLOORPLAN



# EVENING MAPS

## Paris





**FRIDAY NIGHT**

BRENTWOOD BOARDROOM

SANTA MONICA 3

WILSHIRE BALLROOM A

B

SUNSET 4

SUNSET 3

SUNSET 2

SUNSET 1

2

1

ROTUNDA

GREEN ROOM

NORTH TOWER ELEVATORS

BUSINESS CENTER AND CATERING OFFICE

MELROSE 3

MELROSE 2

MELROSE 1

Movie Night

MELROSE 4

AV ROOM

MEZZANINE

Hacker Jeopardy

Who's Slide Is It Anyway?

FIRESIDES

SIN CITY THEATER

THE CHAPEL

SOUTH TOWER ELEVATORS

THE STUDIO

SPA BY MANDARA

Chillout

SecKC

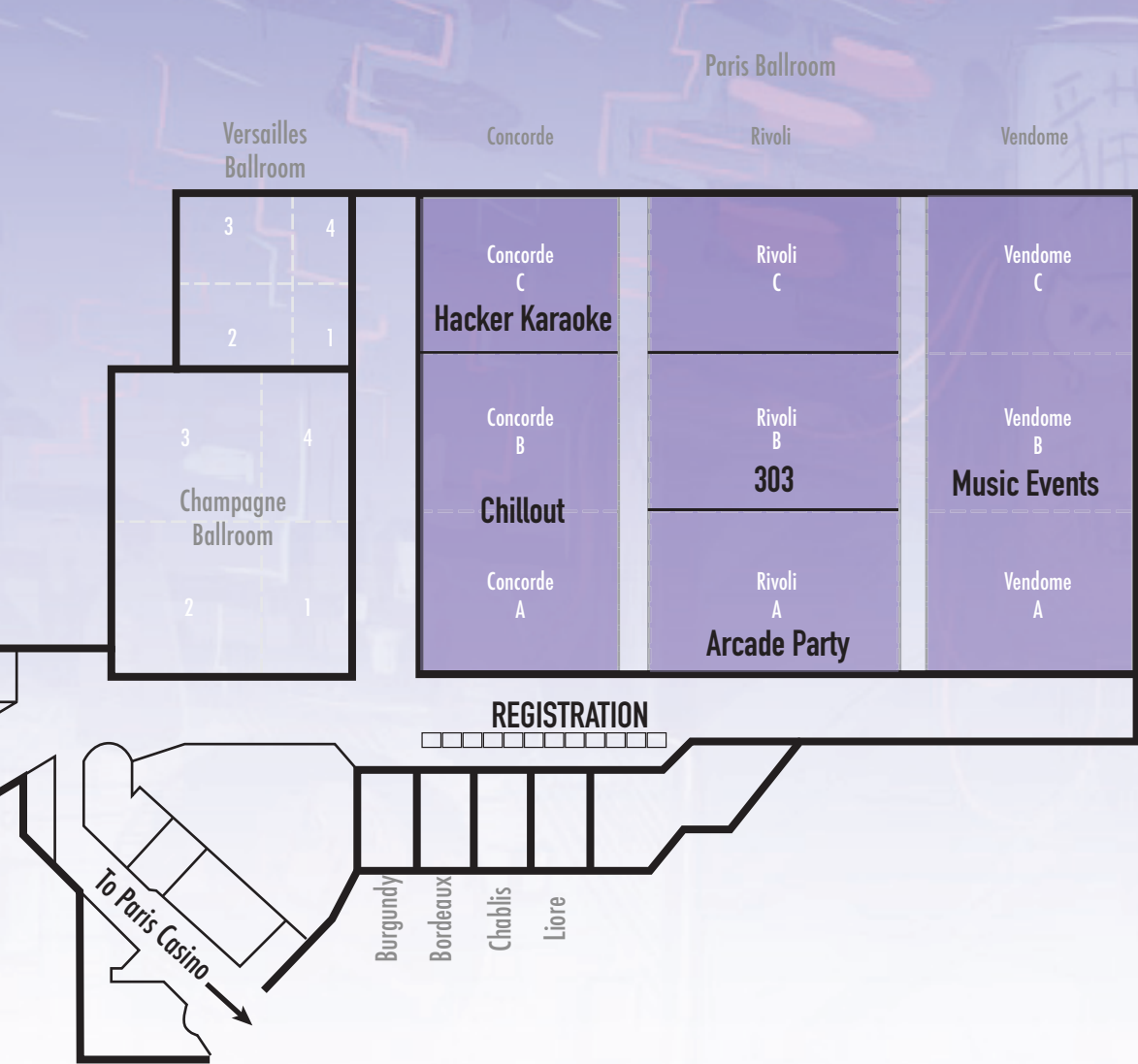
To Showroom and Restaurants

To Casino and Lobby



# EVENING MAPS

## Paris





**SATURDAY NIGHT**

BRENTWOOD BOARDROOM

SANTA MONICA 3

WILSHIRE BALLROOM A

B

ROTUNDA

GREEN ROOM

NORTH TOWER ELEVATORS

BUSINESS CENTER AND CATERING OFFICE

MELROSE 3

MELROSE 2

MELROSE 1

Movie Night MELROSE 4

AV ROOM

MEZZANINE

Hacker Jeopardy

Drunk Hacker History

FIRESIDES

SIN CITY THEATER

THE CHAPEL

SOUTH TOWER ELEVATORS

THE STUDIO

SPA BY MANDARA

Hacker Flairgrounds

GothCon

To Showroom and Restaurants

To Casino and Lobby

SUNSET 4

SUNSET 3

SUNSET 2

SUNSET 1

2

1



# THANK YOU!

Organizing DEF CON happens year-round and sometimes feels it's happening in slow motion, until it feels like it happens all at once. It takes a special kind of team to adapt to the ups and downs. The moments of nothing to do and then the tight deadlines that you stay up all night to meet.

I'd like to thank everyone for believing in and supporting DEF CON over the years – the speakers, contest organizers, the villages large and small, the artists and musicians, and those who helped build our foundation but are no longer with us, for adapting with the times and always surprising me with new ideas and keeping things real. That's what I love most about the con.

To pull it all together I'd like to acknowledge and thank Cayce, Nikita, Neil, Darington, Will, Janet, Linda, Jeff, Number Six, Charel, and Mar. To help coordinate such a large event takes dedicated leaders, and I'd like to thank all the department leads and their #2s listed below. Without them there would be no con.

Finally, I thank each and every Goon, speaker, and organizer that had the courage to help build something bigger than themselves, to take a risk that it might not happen as you planned, and did it anyway. I would jump into a pool with any of you!

-The Dark Tangent

## CFP REVIEW

Nikita would like to thank the DC27 Content Reviewers;

The Dark Tangent, Alex, Nikita, Ash, CyberSulu, Dakahuna, Dino, Beaker, SinderzNAshe, Magen "Tottie", carnal0wnage, Suggy (aka Ninja P14gue), Grant (aka Claviger, FishSupreme), Dead Addict, Highwiz, Jason (aka w0nk, z00mie), Malware Unicorn, Medic, pwcraack, SecBarbie Shaggy, Stephanie (ake Snow), Yan, Zfasel, Zoz, and Tuna, RIP we miss you.

## SPEAKER OPS

pwcraack would like to thank the Speaker Operations staff for another year of great service to DEF CON and its speakers. These goons are Pasties, Crash, Pardus, CLI, Jur1st, Goeke, phliKtid, Bushy, Vaedron, idontdrivecars, K-hole, St0nehouse, notkevin, Flatire, nerfherder, Jutral, Milhouse, g8, DaKahuna, Gattaca, Surreal Killer, RoundRiver, Jinx, Shadow, h1kari, squirrel, Code24, gdead, 404 and AMFY0YO!

## NOC

effffn and DEF CON once again would like to thank our hard-working NOC team for making the conference network, well, work across all the hotels hosting the conference.

Lots of planning, countless emails and a few phone calls precede the crazy-busy week in Vegas.

While many get to enjoy hacker-summer-camp in style, mac, #sparky, booger, CRV, c0mmiebstnd, Dp1i, c7five, Jon2, deadication, musa, wish, johntitor, MikeD and Toph put in long hours in making sure everything worked at least at one point in time and then got them fixed when something (or you) broke it.

If you happen to see one of these folks around, usually at bar that is closest to the NOC, take a minute to thank them and possibly buy them a round of orange whips.

Also, a huge thank you to the nice folks from Caesars IT and Encore for making our lives a bit easier.

## PRODUCTION

Production team sends thank-yous to the Convention Services teams at Planet Hollywood, Flamingo, Paris and Bally's. Randee for her patience, Jayme for her energy and attitude, and last but not least Wendy, who has been an important advocate for DEF CON. A big thank you to the members of the production team and photo corps: Killerspud, ProdGoon\_22, Cannibal, AST Cell, Gillis, metacortex, oADAMo, Amanda, Proctor, Kampf, Spencurai, skyria, sirashrum, Noise, b0t, and Ira!

## CONTESTS & EVENTS

Grifter and panadero would like to thank all of the Contest and Event organizers for their patience and hard work leading up to DC 27. Props go out to the C&E goons and their tireless efforts during the conference to ensure our humans have a great time, stumper, phorkus, phartacus, saltr, heisenberg, apexxor, secove, rugger, m0hgarr, gomer, rcu83d, zero3, vpos, psychotocide and p0lr. Thanks to DT, Will, Linda, Nikita et al... for putting up with us along the way as well as all the other department goons that support our chunk of DEF CON. Final props to Tuna...the heart of a gentle giant, the smile to light up a room. He never knew a stranger and he always knew you...

## VILLAGES

Zantdoit would like to thank Runner-up, Hony, and F4ux for stepping up lead one of the hotels. Having villages across four hotels would not be possible without their support. A huge shoutout to Amlazar, Runner-up, Zant's daughter, and Hony for all their help in keeping me and everything organized. Villages have continued to grow 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 a BIG welcome to the new ones joining the team. Zantdoit and all the village Goons also want to thank the Village leads and organizers for everything they do to make all these great villages possible.

## PRESS

Thank you to all the journalists, bloggers, and podcasters who not only cover the DEF CON community, but contribute something special to it. To all the elected officials, civil servants, and policymakers who took the time to get to know us a little bit better in order to help protect communities in the real-world, thank you.

Dedicated thanks to all the Press & Policy Goons: Alex, Claire, David, Heather, Jeff, Lin, Linda, Monika, and Nicole! This wouldn't happen without you. — <3Wednesday

## VENDORS

Thank you to all the vendor goons – Janet, Lisal33, Redbeard, Pinball, Rob, Sugi, Hexyll, Triple, Gorgonia, Wad, & Rook! Every year is a new adventure!! It couldn't happen without you, and all your efforts!

## DCTV

DCTV thanks our team: Alex, GhostPepper, Hanna, Sandwich, Tuna, and VideoMan.

## AGE

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.



## SOC

Cjunky and tacitus would like to thank: AdaZebra, airfierce, AlphaKilo, Amber, Arc, arcon, Ast0r, Atrayan, baybe\_doll, BeaMeR, bmOnkey, bogaaron, Br1ck, cheronobyl, Chosen1, crazyhrse, cRusad3r, cymike, Dallas, Darkwolf, deelo, DoktorMayhem, dr.kaos, drfed, ducky, echosixx, Emergency Mexican, f0rt1tud3, Faz, FidgetSpinner, Fox, g33kspeed, gadams, gizmo, Glasswalk3r, GodFix, GuardianCosmos, hamster, Harmless, Hattori Hanzo, Havoc, Infojanitor, iole, iv4t, Jbone, John Doll, Juliet Bravo, Junior, Kardec, kerbear, Knox, Krassi, KRS, kruger, LabRat, logicalrock, logkiller, Lordi, M0, M0rph1x, matrix, mauvehed, MIM, Motsu, Mr. M, n1cFury, Nesquik, NextInLine, nohackme, Nothingness, ObiWan666, OneTwo, Oselot, P33v3, Plasma, polish\_dave, prec0re, Priest, Quiet Mike, Rabbit, Randy\_Waterhouse, Ratchet, Raven, Red, redoubt, SAGE, Salem, shuu, Si, Siviak, skiznotic, Sl3dge, Slick, SomeNinja, Sonicos, Spedione, stan, stealth, Synn, TOBIO1, Thirsty Goat, TieFighter, timball, TRINITY, Wasted, wham, whiskey, WHITE CHRIS, WhiteB0rd, wilnix, winx, Wreaktifier, xenophyx, Zapp, zephfrish, zerofux, zombie, Zulu, all this year's noons, and especially all retired SOC Goons. Pax Per Imperium.

## DEMO LABS

DemoLabs would like to thank Contests and Events for their support, Quartermasters for handling the equipment, NOC for setting up the network, and our content and hotel folks for their support.

And of course - all the fantastic and creative hackery goodness the community came up with this year that makes DemoLabs a success! - heisenberg

## REGISTRATION

Registration (Human lead: cstone; Inhuman lead: f1dget) would like thank our staff: Agent X, APT, Chimera, Crackerjack, estebang, falconred, f0nd004u, funnyguy, holmestrix, Joe630, Jup1t3r, Maggie, mcmayhem, Model A, Paranotic, Phear, phreak, Pozer, qumqats, supertechguy, Temtel, UnderTaker, and w0z. Special thanks to SOC, QM, Swag, Info Booth, Production, and the attendees, as always, for their patience.

## DISPATCH

RF and Ahab would like to thank AsmodianX, Taclane, and Voltage Spike for helping to lead the Dispatch team, and also wish to thank the rest of the Dispatch Staff for all their hard work: BonBon, Fosgood, LOG1C, Dymz, Rixon, w00k, dll3ma, Archangel, and miggles.

## SWAG

Secret would like to thank all the Swag goons: Dasha, gLoBuS, rudy, furysama, webjedi, theViking, Loak, gingerjet, themikeconnor, H4zy, Endsu, Zubion, Mr.Katt, D20OwlBear, pelican, Csp3r, 10rn4, Alex, Skyfall, spiggy, Serenity, Bearclaw, Peej, Magnar, Heal, and cillic for all their hard work and all the other departments who make DEF CON possible!

## DEF CON GROUPS

DEF CON Groups would like to thank Will, Darington, Brent White, Jayson E. Street, April C. Wright, Neil K., s0Ups, Casey Bourbonnais, and Tim Roberts for volunteering extensive time throughout the year and for fostering and contributing to the global DCG community. We would also like to thank all the new and existing groups who help keep the DEF CON spirit going throughout the year and around the world!

## WORKSHOPS

Tottenkoph would like to thank the Workshop Review Board, all of whom worked hard to review workshop proposals this year; Neil and Nikita for all of the hard work they do; her amazing team of goons (SinderzNAshe, beaker, 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.

## QM

The tail lights on the C-17 blinked monotonously as it circled Vegas, the rest of the craft in complete darkness to aid night vision, in stark contrast to the gaudy display of The Strip below... There was a sharp "CLICK!" from the speakers in the cargo bay, then a static hiss and a low grumble from 'Uncle' Ira, the captain of this 'Fun Farm of Death' transporter... "OK folks, we've got the green light for HALO, Angels 25! This is no HopNPop so hands off those pilots! Clear skies guys! Have a cool Con! Running in..." So it seems the last minute warning to the Authoritays had fallen on deaf ears. Again. DEF CON was coming back to town, and it was being dropped on them from 25,000 feet... The red light over the gaping maw of the open loading hatch flicked to green and Major Malfunction watched as eta, Buttersnatcher, SunSh1ne, Geo, The Saint, bigezy Seven, Slacker, shell-e, Drimacus, YoungBlood, Waz, Red Ace, Q, ms7821, @SP3ZN4S, helium, alizarinMegalodon, AWildBeard, Sp1kedshell, netza, failOpen, Cell Wizard and justif3y3 trooped past and down into the murky night... With a thumbs up to Janet & Linda, who would shortly start pushing pallet loads of pelicans out behind them, he let his weight topple him forward and out and then he too was plummeting earthwards, trying to make out his crew against the bright lights below... DEF CON 27 is ON, Baby!

## INFO BOOTH

Littlebruzer and Littleroo would like to thank all of the Info Booth goons for passing out bad information and sending the humans in the wrong direction: Otter, 50 Caliber, Aask, algorithm, ARI, Boudica, Bufo Alvarius, Ch3f, Cheshire, Commrade, dLaw, DMONEYGE3K, G1LL3T3, Krav, Lo, madstringer, Maggie, morphotic, N00bz, Nav, Nebberz, Nymphaea Caerulea, Nyx, Paul, Pocket, Razzies, S747IK, Sanchez, SchematicAddict, ScurryFool, SmoOotch, Sparkle, TACSAT, and Viva.

A special shout out to Advice, lawticus, and the rest of the Hacker Tracker Team for their hard work on the mobile applications and the web site.

The entire Info Booth team would like to thank all of the humans for the interesting questions. We really do know where the restrooms are located.

## DESIGN & DEPLOYMENT

Neil would like to thank Mar, Sleestak, & Nikita for help getting this book made. p0sterboy for helping get all these hotels covered in signs. A big thank you to the DEF CON Deployment team: Medic, xaphan, & S4m G0ld for working tirelessly to keep you all properly directed.

## PARTIES

xistence would like to thank all of people who bring the parties and meetups that make DEF CON night time such an amazing place to hang out, learn and hack. Also with great thanks to Pyr0 for his 20 years of service at DEF CON - who is retiring for good this year (or so he says) - and my amazing team: Rickglass, s3gfaulst and Skittles.

