



WELCOME TO DEF CON 25!

Silver Anniversary

DEF CON is part conference and part party, a refuge from Info Sec where we can re-charge and be inspired for the year to come. The theme this year is around community, a glance over the shoulder to acknowledge those who carried us this far, and a look forward to the future we have to live in. A retro glitch tech theme wrapped up in 80s video game colors and modern technology. Learn where we come from, and then chart your own path.

We are in a new hotel and it is far too nice for us. It feels surreal to be where Black Hat spent so many years growing, but there is some symmetry there as well. Caesars now will now have had both the Yin and Yang. We have worked hard to design for day and night activities, growing where possible, and expanding our Info Booth team to have more Goons available to help answer questions and steer you in the right direction. Feel free to ask anyone in a red Goon shirt for help, and if they don't have the answer they can forward you to someone who does.

As I write this a month before you read it I can only guess at what craziness will transpire on the lead up and during the convention. We continue to operate in uncharted waters, much like 25 years ago, both legally and technologically. What constitutes unauthorized access? When if ever are manufactures liable? Are hackers just pointing out problems but not helping fix anything? The difference is now we as a community are in the spotlight and everything around us is accelerating: legislation,

connectivity, and the loss of personal agency over our data and identity.

One thing I am certain of though is that hackers will help point the way through this jungle of self serving marketing speak, technically impossible tech policy, and insecure products to give the public a real view of what is possible and what isn't. It won't be the organized crime groups, vulnerable companies or governments doing this, but instead hackers through a deep understanding of technology that can speak truth to power.

Here is to celebrating our successes, honoring those who couldn't be here with us, and to the next 25 years of being hackers living in the middle of a technological revolution!

The Dark Tangent



NETWORK

Network Instructions:

=====

The DEF CON NOC delivers the cyberz throughout the swanky Ceasar's Palace convention center and the DC TV channels to your hotel rooms.

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

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

Despite the fact that the 802.1x Godz seemed to have smiled at us last year, never forget we're talking about the Wi-Fiz: where radio wavez make packets flow and digital magic makes the communications secure, dodging those pineapples along the way.

Since it's quite possible that something changed in the past 12 months on how all operating systems deal with Wi-Fi, there are might be some devices out there that really do not like 802.1x with PEAP authentication. In particular, for quite a while some Android platforms wouldn't verify the RADIUS server certificate prior to sending the user's credentials to enter the network. And this is not cool.

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

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

For updated information and instructions on how to connect to the Wi-Fi with the n0t-s0-l337 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-l337 linux distro, you should consider a new platform.

For other NOC updates visit <https://www.defconnetworking.org> and also follow us on the twitterz @DEFCON_NOC

INFORMATION

DEF CON TV

Nurse your hangover comfortably watching the presentations in your hotel room.

DC TV brings the DEF CON talks to you. Turn on the TV, grab your favorite beverage of choice and aspirin and don't forget to shower.

<http://dctv.defcon.org> is the spot for all your channel info needs.

The DEF CON Media server is back again!

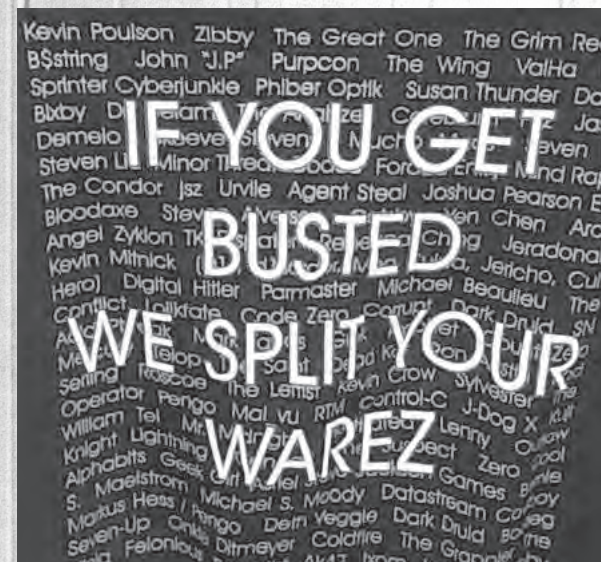
<https://10.0.0.16/> or

<https://dc25-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!

The dc25-media.defcon.org TLS certificate fingerprint:

(SHA1) 52 b2 32 9d 27 28 45 be 88 b8 a9 b7 11 26 b6 13 b4 1c 18 8b



25 YEARS OF DEF CON FUN FACTS

DEFCON V

System Failure Scavenger Hunt

RULES:

FUN FACT: 20 Points for a Live Duck.

OBJECTS:

- | | | | |
|--------|---------------------------------------|--------|---|
| points | object | points | object |
| 60 | Security Camera * | 10 | Pod file to create |
| 20 | Pod file from penguin.com | 10 | Pod file to the |
| 1 | An issue of 2000 * | 1 | # up the Censur |
| 1 | VMI for system failure | 2 | Valid move to |
| 2 | 30 min proposal calling card | 10 | Pod file to make |
| 6 | Amex, full info | 10 | Redecorate w/ |
| 5 | Books from Sprint (Vegas) * | 1 | You have a real |
| 2 | Radio Frequency used by Aladdin | 1 | You let us sleep |
| 1 | Security radon | 2 | You have a plan |
| 2 | Slee machine token | 1 | DefCon |
| 2 | Room key from the Aladdin | 1 | Radon * |
| 10 | Security radio * | 6 | Security Radon |
| 5 | Telco hat or shirt * | 5 | 800/888/8888 PIN |
| 2 | Something related to Area 51 | 1 | San Pedro Cam |
| 1 | Valid conf info (AT&T conf) | 2 | "Hackers" name |
| 5 | Amex or access for System Failure | 5 | Docs from an |
| 3 | You are wearing an "I spotted the | 15 | Pod file to write |
| 3 | Pod" shirt | 8 | Cashed pizza |
| 3 | A Penguin Palace comic book * | 1 | Photo of you in |
| 6 | Street sign * | 4 | Telco hand hat |
| 2 | Movie snafu from MIB (Vegas) * | 5 | Group line with |
| 2 | Valid MIB or Amex | 5 | Convince a kid that you are cool & not "freaky" |
| 10 | Andy Scott (Penguin)'s finger | | with audio video, or bring the kid to the booth |
| 10 | Find a diverter with a 702 ac | | |
| 2 | (800) ANI # | | |
| 5 | (702) ANI # | | |
| 8 | Pod file to CUSUM | | |
| 15 | Redecorate a foreign webpage | | |
| 20 | A live duck * | | |
| 5 | Go on the roller coaster with a drunk | | |
| 8 | at Jada (501 people only) | | |
| 5 | Wav of you harassing OGI | | |
| 10 | Buy 5 System Failure stickers * | | |
| 10 | Buy 10 System Failure stickers * | | |
| 5 | Lineman's handker * | | |
| 20 | Syllabi article for #3 (must be | | |
| 10 | approved by LegiScribe) | | |
| 10 | Dinner for Syllabi editors, social | | |
| 5 | engineered from McDonalds | | |
| 5 | Set an 800/888 # to your hotel room | | |

PRIZES:

As of 7/6/97 we have in our prize box: 4-way sign, cyberpunk novel, Angel Free BSD CD, and door from US West. We plan to have by DefCon a MAC printer, paper from Pacifiell, 2 pg lrd, and a can of SPAM. Winners will be announced on www.penguinplace.com/syllabi and in System Failure #3. There is one prize box for the group to split among themselves.

To claim your prize someone from your group must meet at the System Failure table by 1pm Sunday. If nobody gets 100 points worth of objects, the group with the highest number wins.



FUN FACT: DT STARTED THE TACTICAL TURTLENECK



DC1 COULD HAVE BEEN HELD IN A TINY GERMAN CAR.

FUN FACT: DEF CON II had an official banana. This is a bad picture of that banana.

BONUS FACT: Banana reported missing from headdress at Tropicana stage show

STATUS: Likely unrelated



STILL EPIC

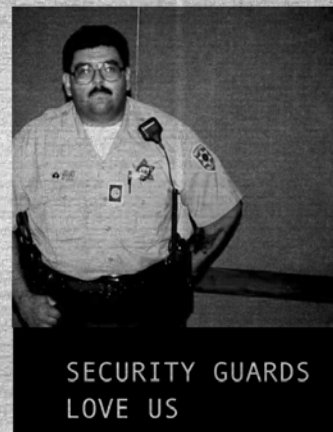


DEF CON LOVES YOU!

FUN FACT: DON'T.



FUN FACT: THIS KID'S SHIRT PROBABLY FITS NOW



SECURITY GUARDS LOVE US



WE DID NOT PREDICT #BADGELIFE



Please Excuse this pile of trash. If you could leave us trash bags - lots of them - we need big trash bags thanks. -1751-sharks and

FUN FACT: THIS IS NOT HOW YOU STAY UNDER THE RADAR



DEF CON IV
LAS VEGAS 1996

In the 90s, Hacker Belts worked TOO Hard.

FUN FACT: THROUGH THE POWER OF DNS, DAN KAMINSKY CAN BILOCATE.

BADGE

Over the years the DEF CON badges have grown from simple laminated designs to highly complex electronic artifacts full of puzzles. I am proud that we were the first to introduce the concept of the Black Badge, or free admittance for life for demonstrating expert hacking skills or ability. Black Beetle did a lenticular badge, a liquid filled badge, and a metal stamped badge, but when I asked King Pin to design an electronic badge for DEF CON 14 he created the now famous smiley skull badge and the electronic con badge wars began. LDstBoy took it to another level by increasing the complexity and uniqueness of the Uber black badges.

After 24 years it actually becomes more difficult, not less, to design and plan the badges. As the con has grown the number of badges grow, and production lead times increase. For example the second year we did electronic badges we purchased every available battery holder of that type in the US market. Planning needs to begin earlier and earlier, and that is what did us in this year. We were at deadline for the badges and the design was not ready, and so we had to switch to plan B. As hackers we always have a plan B.

Nikita and I were talking about plan B, and I wanted to do the first eight years of badges we ever produced as a retrospective and tie into the 25th anniversary theme this year. She came up with a better idea of doing the most interesting or popular badges of the past 24 years. I was thinking of the badges as stitched patches with Velcro on the back but there was not enough time to manufacture them, and Nikita thought of them as giant rubber type key chains and there was time left for that. Winner! We selected the badges, Neil did the art, Nikita sorted out quantities and if all goes well the finished

out quantities and if well the finished badges will arrive on site with a few days to spare. Here is their history:

DEF CON 1

In 1993, I sketched the first DEF CON logo while at Dead Addict's place. (It was refined in corel draw and produced in a continuous tone printing process from a Fiery RIP, in the only place that could do such printing in Seattle in 1993. Overtime the logo grew and changed, the icons went from 1 to 4, but this was the first. Like how there are spaces for your handle and group affiliation? Things of the past.

DEF CON 5

The "Area 51" badge. It wasn't the first Goon Staff badge, but I went through a lot of trouble to make these look like cool official Gov't badges as possible.

I used limited edition florescent inks printed on a Canon tabloid printer and hand cut and laminated at a local Kinkos.

DEF CON 7

The first all metal badge done in aluminum. This was also a "Plan B" badge and a rush job. We payed crazy rush fees at a local Seattle company that also makes signage for companies such as Boeing and IBM, but the result was great. We have done a other metal badges of various degree of difficulty since, but these were the first.

DEF CON 9

The liquid filled squishy badge designed by Black Beetle. If you're lucky enough to have one of these original badges, I envy you. This was a brand new manufacturing process and we took a risk on them. Would they pop? Leak? The cool factor was worth it and they turned into one of our most iconic badges. One of the more difficult badges to counterfeit during the con. I've been looking for something similarly cool ever since.

DEF CON 12

The rocket ship badge that year had its own cool design by Black Beetle. It again as a new production process with clear material, color, and silver foil stamping in a custom die cut shape. The art was inspired by Ghost in the Shell.

DEF CON 14

The iconic first electronic badge by KingPin. While simple in design these badges were awesome. They used brand new PCB colors to designate different departments, and we even did a limited run of them using gold for masking, the first time it was ever done by the manufacturer! At closing ceremonies we turned off the lights and the room glowed as we played a song created during the badge hacking contest and it was like a being at a concert of your favorite band. The feeling of community was amazing. You can listen to the song by downloading it from the https://dc25-media.defcon.org/media_server.

DEF CON 17

With art design by Neil and engineering from Kingpin the electronic puzzle badge was the first designed specifically to get all the attendees to seek out and interact with each other in an attempt to assemble and wire it up. You had to get ALL the pieces together, including a super rare Uber badge, to form the whole circle and circuit. Since then we always think of ways to use the badges to get DEF CON hackers to work together to solve a problem.

DEF CON 19

The Uber titanium skull badge by L0stBoy. Just look at it, it's cool, it's tough, it's not breaking anytime soon. Going all "Maker" on us L0st went with a more difficult tempering

process that produces one of a kind multi-color finish. If you see someone with one check it out under a bright light to see what I mean.

I don't have enough room on this page to list them all, and who knows, the remaining ones might be needed for a "Plan C" one day. To check out a collection of almost all past badges, browse to Grifter's collection here: <http://www.rootcompromise.org/gallery/v/defcon/dcbadges/>

The Dark Tangent

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 25

Caption Contest

Tweet your caption ideas.
Use the appropriate hashtag.
Chuckle. Share. Repeat.



#DefCap_DT



#DefCap_DanFarmer



#DefCap_rman



#DefCap_rascal

What is DT thinking?

What is going on
with Mr. Farmer?

What naughty spell
did that wizard just
cast?

The world awaits
your answers.

follow DEF CON AT
@DEFCON and @DCIB



#DefCap_wizard

GOONSPOTTING

HOW TO SPOT A GOON:

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:

- 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 25 Goon shirt, and they will also be wearing a current year Goon badge. If they are not wearing both then they are not on duty.

- Goons on duty are not supposed to drink alcohol.

- All Goons off duty are NOT to wear their red Goon shirt to prevent confusion with attendees and give them a change to not be approached with con related issues. Goons in this state have been known to drink alcohol.

- PAST Goons may seen wearing previous red shirts or badges and they helped run a past DEF CON, but that does not make them a current DEF CON 25 Goon.

- On almost all the Goon shirts there is a department name on the back of the shirt to tell you what group you are dealing with. Please use this if you have any feedback on Goons, both good or bad. It was not logistically possible to add individual name or handles this year, but we will at DC 26 (Feedback can be sent to feedback@defcon.org)

- Goons goon for many reasons, but the pay isn't one of them. They put in long hours and many weeks or months of planning and take time off work to make the con happen.



(The shirts & badges will be red)

EVENING LOUNGES

Introducing DEF CON Evening Lounges

These are smaller more intimate talks that don't require audio and video support for a limited audience. For more detailed descriptions view their abstracts in the presentation pages.

Panel - An Evening with the EFF

Friday at 20:00 - 22:00 in Trevi Room

Hacking Democracy, with Mr. Sean Kanuck

Friday at 20:00 - 22:00 in Capri Room

Horrer stories of a translator and how a tweet can start a war with less than 140 characters, with El Kentaro

Friday at 20:00 - 22:00 in Modena

Panel - Meet the Feds (who care about security research)

Saturday at 20:00 - 22:00 in Capri Room

Panel - DO No H4RM: A Healthcare Security Conversation

Saturday at 20:00 - 22:00 in Modena Room

THE FUTURE OF DEF CON

THE FUTURE OF DEF CON

When I started DEF CON the only hacker cons I knew of were SummerCon and HoHoCon, 25 years later there are hundreds of security related cons ranging from pure hacker to career oriented Info Sec industry events. From small to large, invite only to open and specific to general there is more than something to meet everyone's interests. Where does DEF CON fit in?

I have been thinking a lot since DEF CON 20 about the future of the con, and while I don't have a crystal ball of what is to come I do have some conclusions:

Last year I wrote "DEF CON is a hacker con, not an Info Sec conference. I bring this up because there is a difference, one is more focused on joy of discovery, irreverence, novel, if impractical approaches. The other is more focused on enterprise solutions, frameworks, and concerns large companies may have.. There is great value in the different types of conferences, and if this con doesn't feel like others it is by design.."

This is the lens with which the review board looks at all submissions. Sometimes we have to pass on a fantastic submission because DEF CON is not the right venue. Knowing this gives us focus and sets expectations for attendees. Activities that enable the hacker mindset and demonstrate how to master a certain technique are always going to be selected over a great enterprise security talk.

Over the years speakers, organizers, villages and staff come and go. What is important is for the con to remain an open platform for new ideas. DEF CON must not only invite back popular and well run villages and events but also take risks on new ideas. For example the Car Hacking village was an untested idea a few years ago, now they are well established. This year we are trying a new Voting Machine Hacking Village, something not done before. As Jericho once said years ago DEF CON is really a convention of mini-conventions, and by offering space and encouraging risk taking DEF CON will constantly renew itself.

DEF CON can happen more than once a year in various forms. For two years we ran some of the hacking villages at the Tibeca Film Festival and reached a whole new audience interested in hacking, technology, and privacy. It was a great experience and hopefully some writers and directors will look at hacking

differently. Don't be surprised if parts of DEF CON do future road trips to bring our hacking to other communities.

DEF CON is a business, but behaves much of the time like an association. We don't take pre-registration because we value your privacy, even if it makes guessing how many people to expect and materials to purchase difficult. We don't take sponsorship because it doesn't feel right, like some innocence would be lost and a bunch of expectations would be added, our neutrality compromised. Sometimes keeping it hacker isn't the most efficient business decision, but DEF CON would not exist without the support of the hacking community and that needs to be continuously respected.



DEF CON 25 ALL-NIGHT

MUSIC LINEUP!

MAINSTAGE

THURSDAY

2100 - 2200 - DIDEAD
2200 - 2300 - SKITTISH AND BUS
2300 - 0000 - ACID T
0000 - 0100 - REID SPEED
0100 - 0200 - NINJULA
0200 - 0300 - SCOTCH AND BUBBLES

Reel
Big Fish



zee

ZEBBLER ENCANTI EXPERIENCE

DRESS UP NICE AND JOIN US!

FRIDAY

2100 - 2230 RICHARD CHEESE (CHILLOUT AREA)
2230 - 2300 DUALCORE
2300 - 2330 MC FRONTALOT
2330 - 0000 YT CRACKER
0000 - 0130 REEL BIG FISH
0130 - 0200 KRISZ KLINK

SATURDAY

2100 - 2200 MODERNS
2200 - 2300 JACKALOPE
2300 - 0000 ZEBBLER ENCANTI
2330 - 0000 LEFT/RIGHT
0000 - 0130 KILL THE NOISE
0130 - 0200 CTRL/RSM

MC
frontalot

ytcracker
THE ORIGINAL, DIGITAL GARGOYLE



<dualcore>

BIOHACKING VILLAGE



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's 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.

DIY BioHacking Philosophy Like all hackers, we are looking to subvert the dominant paradigm...of life itself. Our village will excite, elucidate, enlighten, and engage participants in the technical, mechanical, procedural, and human side of biohacking.

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

CAR HACKING VILLAGE



Car Hacking Village is an interactive, hands-on village with the goal of teaching village goers what car hacking is, introducing village goers to the tools of car hacking, and working with hackers to create a community of car hackers at Def Con 25.

We will bring back our Car Hacking CTF this year, please go

to CarHackingVillage.com for sign-up information.

This year we will split the village into Zones:

* **Driver Information Zone** will orient village goers on the events, talks, and contests that we'll be running as well as introducing village goers to organizations that are moving Car Hacking forward.

* **Brake-It Zone** will be a hands-on pull-apart area where village goers can disassemble vehicle trim panels and connect to vehicle wires. Here we will have a new contest this year we are calling the Trunk Escape Room. Please check the car hacking village web page for more details on how to sign up.

* **Buck Hacking Zone** will be hands-on electronic module hacking area where village goers will come to learn how to send commands to electronic modules from vehicles. We will have hardware and computers available, but feel free to bring your own as well.

* **Turbo Talks Zone** will be 15 to 20 minute talks about car hacking techniques. Visit CarHackingVillage.com for an updated schedule.

* **OEM Zone** will be where you can meet the automakers and play the vehicle simulator game.

Please check the CarHackingVillage.com web page for more up-to-the-date information. Please follow @CarHackVillage on twitter for live details during Def Con 25.

Friday 1000 - 2000, Saturday 1000 - 2000, Sunday 1000 - 1500

CRYPTO AND PRIVACY VILLAGE



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, a key-signing party, and other TBD awesomeness.

Friday 1000 - 1800, Saturday 1000 - 1800, Sunday 1030 - 1400

DATA DUPLICATION VILLAGE



Last years DEF CON data duplication village was a massive success with about 2 Petabytes of data duplicated. Let's do it again!

HOW IT WORKS DEF CON will provide a core set of drive duplicators as well as data content options. It will be a first come, first served and duplicate 'till we drop. Bring labeled 6TB SATA blank drives, and submit them in the queue for the data you want. Come back in 14-24 hours to pick up your data-packed drive. Space allowing, the last drop-offs will be no later than Saturday afternoon and the last drives will run overnight with the final pickup time at 11:30am.

WHAT YOU NEED - 6TB SATA3 new drive(s) - If you want a full copy of everything you will need three. Be aware that we cleared all of Vegas of 6TB drives last year so get them early!

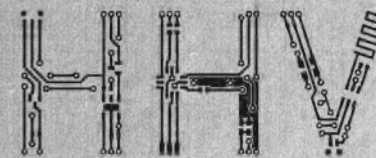
WHAT YOU GET We're still working out the details but this is what was provided for DC24... - 6TB drive 1-3: All past hacking convention videos that DT could find, built on last years collection - 6TB drive 2-3: freerainbowtables.com hash tables (1-2) - 6TB drive 3-3: GSM A5/1 hash tables plus remaining freerainbowtables.com data (2-2)

SIDE NOTES duplicating a 6TB (About 5.46 usable) drive at an average of 120 Megabytes a second comes out to just under 14 hours per drive. With about 16 duplicators doing about 95 drives concurrently, we expect push about 11GB per second out to the drives to try to meet demand. We did 335 drives for DC24 and we're hoping to do even more this year!

Welcome to Vegas!

Thursday 1700 - 2000, Friday 1000 - 2000, Saturday 1000 - 2000, Sunday 1000 - 1200

HARDWARE HACKING VILLAGE



The DEF CON Hardware Hacking Village celebrates its OxA anniversary! Come join us for hardware

hacking, teaching, learning, and exploration.

Lots of prizes to go around, and lots of puzzles to learn new things or show off your skills.

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

IoT VILLAGE



IoT Village is back for the third year at DEF CON. Organized by security consulting and research firm Independent Security Evaluators (ISE), the IoT Village delivers advocacy for and expertise on security advancements in Internet of Things devices. IoT Village hosts talks by expert

security researchers who dissect real-world exploits and vulnerabilities and hacking contests consisting of off-the-shelf IoT devices.

IoT Village's contests are brought to you by SOHOpelessly Broken™, the first-ever router hacking contest at DEF CON. The ISE research that inspired the SOHOpelessly Broken™ contests delivered 56 CVEs to the infosec community. Over the years at DEF CON, IoT Village has served as the platform to showcase and uncover 113 new vulnerabilities in connected devices.

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

Friday 1000 - 1800, Saturday 1000 - 1800, Sunday 1000 - 1500

ICS VILLAGE

A small group of SCADA Ninjas are travelling around the globe, spreading the word of SCADA. Unless you are already operating a secret nuclear enrichment facility in your basement or an ACME factory production line, then this is your best chance to get a kick-start into the world of Industrial Control Systems. We are bringing a number of real-world industrial devices from different vendors for you to look, feel and mess around with.

We bring you a safe, yet realistic environment where you can learn on how to assess, enhance, and defend your Industrial Environment. We bring you real components such as Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), Remote Telemetry Units (RTU), Actuators, and miniature robotic arms, to simulate a realistic environment by using common components throughout different industrial sectors.

You will be able to connect your machine towards the different industrial components and networks and try to assess these ICS devices with common

security scanners, network sniffers to sniff the industrial traffic, and more! If you are new to the world of Industrial Controls Systems, don't be shy! We are more than happy to teach and answer any questions you may have!

Friday 1000 - 1700, Saturday 1000 - 1700

LOCKPICK VILLAGE



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.

Friday 1000 - 1800, Saturday 1000 - 1800, Sunday 1000 - 1500

RECON VILLAGE

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, 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.

Following events will be hosted within the village:

Keynote by Shane McDougall (@tactical_intel)

An OSINT CTF that runs throughout the village timings.

Talk Formats:

Comprehensive Talks (30-45 minutes)

Lightening Talks (10-20 minutes) and

Live Demos (20-30 minutes)

2 Hands on OSINT Workshops (2 Hours each)

Friday 1400 - 1900, Saturday 1000 - 1830 Sunday 1000 - 1200

ROOTZ ASYLUM

"rootz 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,

VILLAGES

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."

Friday 1000 - 1700, Saturday 1000 - 1700 Sunday 1000 - 1500

SKYTALKS 303

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

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

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

Friday 0900 - 1900, Saturday 0900 - 1900 and 303 party door at 2230

TAMPER EVIDENT VILLAGE

"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 Tamper-Evident Village is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

Friday 1000 - 1800, Saturday 1000 - 1800, Sunday 1000 - 1500

THE SOCIAL ENGINEER VILLAGE



Established at DEF CON 18 the SE Village has been the one-stop shop for all things social engineering

at DEF CON. From our humble beginnings with a small room and our sound proof booth to now running 5 events and a "Human Track" where top quality and hand chosen social engineering talks are given.

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

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

Thursday 1000 - 1700, Friday 1000 - 2000,

Saturday 1000 - 2000, Sunday 1000 - 1200

VOTING MACHINE HACKING VILLAGE

Announcing the Voting Machine Hacking Village @ DEF CON 25

When: Friday & Saturday, 10:00 to 17:00. Sunday 10:00 to 14:00

Where: Anzio on the Promenade level.

CONCEPT: Get a bunch of voting machines and start hacking on them to raise awareness and find out for ourselves what the deal is. We're tired of reading misinformation about voting system security so it is time for a DEF CON Village...

Until now getting access to real voting machines has been almost impossible. The public has been assured by the vendors that the systems are safe, but who can verify that? The DEF CON Voting Machine Hacking Village provides you access to real voting machines, used in past elections and to be used in future elections. We'll have over 50 machines of different types to play with!

Now we, as community, can take a look ourselves and asses the security of these systems and help general public to get educated and the policy makers to get old-fashioned facts.

As a first year Village we will get everyone started on understanding the technology and systems these machines live in. By year three we hope to have a complete functioning stand alone voting network that we can test. Believe it or not no such network has ever been security tested or audited - only separate pieces.

THREE MODES: We will go at this three different ways for year one.

- Build a network and have network monitoring ports where people can play "Man in the Middle" or other active attacks to simulate an attacker at distance.
- Have active stand alone systems and see what physical attacks are possible.
- Hardware hack on the machines, dump their BIOS, EEPROMs, reverse engineer what we can, and generally learn what we can of how they are built and the quality of the code running on them.

We will try to capture as much information and results as possible and try to create a report in the end of our experiences to help others who want to continue the work. We'll be working towards getting the back end systems and software necessary to build a complete network as a goal for next year.

VerifiedVoting will also have a table in the vendor area and be present to help educate everyone who may have questions.

The Dark Tangent would like to thank Harri Hursti and Matt Blaze for their help running the village. They are subject matter experts with years of experience in voting technology. For more information and to stay connected on our village check us out at <https://forum.defcon.org/>

VOTING VILLAGE SPEAKING TRACK

When: Friday, 10:00 to 17:00

Where: Roman 1 on the Promenade Level.

10:00 - 10:45

Barbara Simons, Chairwoman, Verified Voting

An election system is much more than the voting machine or the booth, overview of the election IT systems, the threat models and procedural safeguards.

Barbara Simons is a computer scientist and past president of the Association for Computing Machinery (ACM). She is founder and former Chair of USACM, the ACM U.S. Public Policy Committee. Her main areas of research are compiler optimization and scheduling theory. Together with Douglas W. Jones, Simons co-authored a book on electronic voting entitled Broken Ballots.

Since at least 2002 Simons has been a critic of unauditable electronic voting and is generally credited as a key player in getting the League of Women Voters to change its stance on this issue. Initially the League had seen electronic voting mainly as a way to minimize invalidly cast ballots, but at their June 2004 convention she led a successful fight to get this policy reversed to one of giving priority to voting machines that are "recountable".

She was a member of the National Workshop on Internet Voting that was convened at the request of President Clinton and produced a report on Internet Voting in 2001. She also participated on the Security Peer Review Group for the US Department of Defense's Internet voting project (SERVE) and co-authored the report that led to the cancellation of SERVE because of security concerns. Simons co-chaired the ACM study of statewide databases of registered voters. She recently co-authored the League of Women Voters report on election auditing. In 2008 she was appointed to the Election Assistance Commission Board of Advisors by Senator Harry Reid.

11:00 - 11:45

Introduction into hacking the equipment in the village.

12:00 - 12:45

Joe Hall

Legal considerations of hacking election machines.

13:00 - 13:45

Harri Hurst

Brief history of election machine hacking and lessons learned so far and why it is hard to tell the difference between incompetence and malice.

Harri Hursti is a Finnish computer programmer and former Chairman of the Board and co-founder of ROMmon where he supervised in the development of the world's smallest 2 gigabit traffic analysis product that was later acquired by F-Secure Corporation.

Hursti is well known for participating in the Black Box Voting hack studies, along with Dr. Herbert "Hugh" Thompson. The memory card hack demonstrated in Leon County is popularly known as "the Hursti Hack". This hack was part of a series of four voting machine hacking tests organized by the nonprofit election watchdog group Black Box Voting in collaboration with the producers of HBO documentary, Hacking Democracy. The studies proved serious security flaws in the voting systems of Diebold Election Systems.

14:00 - 14:45

General Doug Lute, Former U.S. Ambassador to NATO.

The governments can be changed by bullets or ballots, International and domestic interest to interfere.

General Douglas Lute is a U.S. public servant who served as the United States Permanent Representative to NATO from 2013 to 2017.

15:00 - 15:45

Common misconceptions and false parallels about voting technology. We can do online banking and use ATMs, why can't we vote on touch screens or online?

16:00 - 16:45

Matt Blaze

How did we get here: A history of voting technology, hanging chads, and the Help America Vote Act. I'll bring a punch card machine and demo what can go wrong with it. Friday 1000 - 2000, Saturday 1000 - 2000, Sunday 1000 - 1500

WIRELESS VILLAGE



The Wireless Village is a group of experts in the areas of information security, WiFi, and radio frequency with the common purpose to teach the exploration of these technologies. We focus on teaching classes on Wifi and Software Defined

Radio, presenting guest speakers and panels, and providing the very best in Wireless Capture the Flag (WCTF) practice to promote learning.

The Wireless Village plans to hold a Wireless Capture the Flag (WCTF) contest during DEF CON. We cater to those who are new to this game and those who have been playing for a long time. Each WCTF begins with a presentation on How to WCTF. We also have a resources page on our website that guides participants in their selection of equipment to bring. The Wireless Village is also be running a speaker track again. Full updated schedule can be found on our website. Keep an eye on @wctf_us and @WIFI_Village

LINKS: Check out our website for tools, what you need, and what to do. Enjoy your journey. <http://wirelessvillage.ninja> and <http://sdr.ninja/>

We have a number of people who support the Village and staff BIOs are shown on our website. <http://www.wirelessvillage.ninja/crew.html>

Tools/tips

<http://www.wirelessvillage.ninja/resources.html>

<http://sdr.ninja/training-events/sdr-wctf/>

Friday 1000 - 2000, Saturday 1000 - 2000, Sunday 1000 - 1500



PARTY!

THURSDAY

n00b Party hosted by Duo Security.

Come to the DC101 Panel, Thursday, Track 1, 16:00 to 17:45 to find out more about this awesome event. All are welcome, but DEF CON "n00bs" are especially encouraged to attend. If you're new to attending DEF CON and are looking to make some connections then this is your party. Music, free swag giveaways, and more!

When: 18:30 - 20:30

Where: Track 4, Octavius Ballroom, Promenade South Level

Thursday Official DEF CON Welcome Party

Come hang out and listen to some awesome music hosted by DEF CON.

Where: Track 1

When: 21:00 - 03:00

FRIDAY

Silent Disco : Party like a Hacker

Free party open to anyone, bring your booze from the bar next door, bring a phone, bring headphones. #PartyTime

Where: Modena, Promenade level

When: 22:00 to 03:00, Friday

INFOSEC UNLOCKED

INFOSEC UNLOCKED will be hosting a safe and fun board game party for DEF CON attendees. We will provide the space, light refreshments and network opportunities -all we need is you! Come learn about what it takes to become a conference speaker; no experience required and ALL are welcome! More details at <https://isunlocked.com/dc25party!!>

Where: Turin, Promenade Level

When: 22:00 to 03:00, Friday

"DCG" Mixer

Come meet the DEF CON Groups organizers after their talk (17:00 - 17:45 in Track 2) on Friday. This DEF CON Groups mixer is for all who are, or want to become, members of local DEF CON Groups. Come to get info, meet peers, and get some DCG swag. There will be a limited amount of free beer via kegs courtesy of The Dark Tangent.

Where: Chillout Lounge, Promenade Level

When: 18:00 to 20:00, Friday

SATURDAY

303 Party

Hosted and produced by the hacker collective simply known as "303".

Also ...

When: 22:30 to 03:00

Where: Promenade level, in Skytalks room.

FRIDAY & SATURDAY

Hacker Karaoke

Our 9th year! Celebrate with us and with others who love sing. Do you like music? Do you like performances? Want to BE the performer? Want to have that "Hold my beer moment" do your best and not injured? Well trot your happy ass down to Hacker Karaoke, DEFCON's on-site karaoke experience. You can be a star, or if you don't want to be a star, you can also take pride in making an utter fool of yourself.

When: Friday & Saturday - 2000-0200

Where: Roman 1, Promenade Level

DEF CON Official Entertainment:

See the entertainment page in this program for more info on our headliners & entertainment schedule.

When: Friday & Saturday, 21:00 to 03:00

Where: Track 1 & Chillout lounges

SEE THE NOCTURNAL MAP ON PAGE 81 FOR A MORE VISUAL DISPLAY OF LOCATIONS



PACKET HACKING VILLAGE

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: Right behind the vendor area!

PACKET HACKING VILLAGE



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

Wall of Sheep gives attendees a friendly reminder to practice safe computing through strong end-to-end encryption. Wall of Sheep Speaker Workshops delivers high quality content for all skill levels. Packet Detective offers hands-on exercises to help anyone develop or improve their Packet-Fu. Sheep Hunt is an exciting wireless competition where anything wireless goes and catching sheep is the goal. Sheep City is back again, with a collection of everyday devices available for you to hack. WoSD/Co 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 six of the seven years of it's run.

Read on to see all of our events!



/wallofsheep



@wallofsheep





CAPTURE THE PACKET

Capture The Packet - CTP

The time for those of hardened mettle is drawing near; are you prepared to battle? Compete in the world's most challenging cyber defense competition with a newly revamped UI and an improved ladder system based on the Aries Security training simulator. In order to triumph over your competitors, contestants must be well rounded, like the samurai. Tear through the challenges, traverse a hostile enterprise class network, and diligently analyze what is found in order to make it out unscathed. Not only glory, but prizes await those that emerge victorious from this upgraded labyrinth.

The Dark Tangent has asked that we extend your time in the labyrinth and this has caused the difficulty of challenges to be amplified, so only the best prepared and battle hardened will escape the crucible. Follow us on Twitter or Facebook (links below) to get notifications for dates and times your team will compete, as well as what prizes will be awarded.

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

WALL OF SHEEP

Wall Of Sheep

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

SHEEP HUNT

Sheep Hunt

Help! Some of our sheep got out of the barn!!! Do you have the skills necessary to track them down and get them back in? This challenge is open to all skill levels, and has something for everyone! So swing by, break out your RF gear, and start looking for transmitting signals... If it can transmit RF, it is probably part of the challenge.

Register and obtain contest instructions and preliminary clues at the Sheep Hunt table or the Packet Hacking Village Info Booth.



WoSDJCo

Wall of Sheep DJ Community - WoSDJCo

Deep, underground house, techno, breaks, and DnB beats mixed live all weekend by your fellow hacker DJs provide the soundtrack for your PHV hax.

Schedule and sounds available at: <https://wallofsheep.com/pages/dc25>

PACKET DETECTIVE

ARIES SECURITY

Packet Detective

Are you interested in learning the art of network analysis, sniffing, or forensics? Do you want to understand the techniques people use to tap into a network, steal passwords and listen to conversations? Packet Detective 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.



SHEEP CITY

Sheep City

Come attempt to hack our Sheep City! It's comprised of the sort of everyday devices found in your home or office, waiting to be turned against you at any moment. Many devices have RF capabilities, so bring your arsenal of tools. And remember... you can't spell "Idiot" without IoT!

Visit the Packet Hacking Village behind the vendor area to obtain the rules and enter the challenge.



HONEY POT

Honey Pot

Over at the Emerging Threats area of the Packet Hacking Village, we are demonstrating the many creative ways that deception systems can enhance your security posture. Hidden among the innocent users of the DEF CON unsecured network lurks a number of vulnerable systems. Compromise the systems, find the clues, solve the puzzle, and claim your prize. Be warned, there are also honeypots meant to distract and disrupt your efforts!



PHV TALKS

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

Updated schedule available at: <https://wallofsheep.com/pages/dc25>



PHV WORKSHOPS

PHV Workshops

New this year, we have 30 laptops available for hands-on labs and training sessions from an amazing line-up of instructors covering beginner to advanced level material. See our website for updated schedules.



PHV TALKS

Schedule and speaker bios available at: <https://wallofsheep.com/pages/dc25>

Friday, July 28th

10:10 - 11 AM:

Opening Ceremony / How Hackers Changed The Security Industry

Chris Wysopal, CTO and Co-Founder of Veracode (@WeldPond)

Before hackers got involved in cybersecurity, the industry was focused on products and compliance. Security was security features: firewalls, authentication, encryption. Little thought was given to vulnerabilities that allowed the bypassing of those features. Gene Stafford famously said SSL between two PCs is like using an armored car to deliver money from one park bench to another. Hackers came along with the idea that you use offensive techniques to simulate how an attacker would discover vulnerabilities in a networks, a system, or an application. Offensive skills have been on the rise ever since and now the best way to secure something it to try and break it yourself before the attacker does.

Attendees will learn why we need the kind of tools hackers build to secure our systems and why we need people who are taught to think like hackers, ‘security champions’, to be part of software development teams.

11:10 AM - 12 PM: When the Current Ransomware and Payload of the Day (CRAP of the day) Hits the Fan: Breaking the Bad News

Catherine Ullman, Senior Information Security Analyst at University at Buffalo (@investigatorchi)
Chris Roberts, Chief Security Architect at Acalvio Technologies (@sidragon1)

Enabling better communications between geeks and management. As humans, we have had 60,000 years to perfect communication, but those of us working in IT, regardless of which side (Blue or Red Team), still struggle with this challenge. We have done our best over the centuries to yell “FIRE!” in a manner befitting our surroundings, yet today we seem utterly incapable of providing that very basic communication capability inside organizations.

This talk will endeavor to explain HOW we can yell “FIRE!” and other necessary things across the enterprise in a language both leadership, managers and end-users understand.

12:10 - 1 PM: Iron Sights for Your Data

Leah Figueroa (@Sweet_Grrl)

Data breaches have become all too common. Major security incidents typically occur at least once a month. With the rise of both security incidents and full data breaches, blue teams are often left scrambling to put out fires and defend themselves without enough information. This is something that can be changed with the right tools. Tools now available allow blue teams to weaponize data and use it to their advantage.

This talk reviews frameworks for clean, consistent data collection and provides an overview of how predictive analytics works, from data collection to data mining to predictive analytics to forecasts. This allows the blue team to focus on potential risks instead of trying to put out every fire.

1:10 - 2 PM: CVE IDs and How to Get Them

Daniel Adinolfi, Lead Cybersecurity Engineer at The MITRE Corporation (@pkdan14850)

Anthony Singleton, Cybersecurity Engineer at The MITRE Corporation

The Common Vulnerabilities and Exposures (CVE) program uniquely identifies and names publicly-disclosed vulnerabilities in software and other codebases. Whether you are a vulnerability researcher, a vendor, or a project maintainer, it has never been easier to have CVE IDs assigned to vulnerabilities you are disclosing or coordinating around. This presentation will be an opportunity to find out how to participate as well as a chance to offer your thoughts, questions, or feedback about CVE. Attendees will learn what is considered a vulnerability for CVE, how to assign CVE IDs to vulnerabilities, how to describe those vulnerabilities within CVE ID entries, how to submit those assignments, and where to get more information about CVE assignment.

2:10 - 3 PM: You’re Going to Connect to the Wrong Domain

Sam Erb (@erbbysam)

Can you tell the difference between google.com and google. com? How about xn--ggle-55da.com and google.com? Both domain names are valid and show up in the Certificate Transparency log. This talk will be a fun and frustrating look at typosquatting, bitsquatting and IDN homoglyphs. This talk will cover the basics, show real-world examples and show how to use Certificate Transparency to track down particularly malicious impersonating domain names which have valid X.509 certificates.

3:10 - 4 PM: IP Spoofing

Marek Majkowski, Cloudflare (@majek04)

At Cloudflare we deal with DDoS attacks every day. Over the years, we’ve gained a lot of experience in defending from all different kinds of threats. We have found that the largest attacks that cause the internet infrastructure to burn are only possible due to IP spoofing.

In this talk we’ll discuss what we learned about the L3 (Layer 3 OSI stack) IP spoofing. We’ll explain why L3 attacks are even possible in today’s internet and what direct and reflected L3 attacks look like. We’ll describe our attempts to trace the IP spoofing and why attack attribution is so hard. Our architecture allows us to perform most attack mitigations in software. We’ll explain a couple of effective L3 mitigation techniques we’ve developed to stop our servers burning.

4:10 - 5 PM: Layer 8 and Why People are the Most Important Security Tool

Damon Small, Technical Director, Security Consulting at NCC Group North America (@damonsmall)

People are the cause of many security problems, but people are also the most effective resource for combating them. Technology is critical, but without trained professionals, it is ineffective. In the context two case studies, the presenter will describe specific instances where human creativity and skill overcame technical deficiencies. The presenter believes this topic to be particularly relevant for the Packet Hacking Village, as many techniques used are the same that are pertinent for Capture the Packet and Packet Detective.

Technical details will include the specific tools used, screenshots of captured data, and analysis of the malware and the malicious user’s activity. The goal of the presentation is show the importance of technical ability and critical thinking, and to demonstrate that skilled people are the most important tool in an information security program.

5:10 - 6 PM: AWS Resistance and lateral Movement Techniques

AWS Resistance and Lateral Movement Techniques

Peter Ewane, Security Researcher at AlienVault (eaterofpumpkin)

The use of Amazon Cloud as a base of operations for businesses is increasing at a rapid rate. Everyone from 2 person start-ups to major companies have been migrating to the cloud. Because of this migration, cloud vendors have become the focus of potential exploitation and various role abuse in order to achieve persistence. This presentation will cover several different methods of post-infection and account persistence along with a discussion on best practices that can be used to protect from such techniques.

Saturday, July 29th

10:10 - 11 AM: Make Your Own 802.11ac

Monitoring Hacker Gadget

Vivek Ramachandran, Founder of Pentester Academy and SecurityTube.net (@securitytube)

Thomas d’Otreppe, Author of Aircrack-ng (@aircrackng)

802.11ac networks present a significant challenge for scalable packet sniffing and analysis. With projected speeds in the Gigabit range, USB Wi-Fi card based solutions are now obsolete! In this workshop, we will look at how to build a custom monitoring solution for 802.11ac using off the shelf access points and open source software. Our “Hacker Gadget” will address 802.11ac monitoring challenges such as channel bonding, DFS channels, spatial streams and high throughput data rates. We will also look at different techniques to do live streaming analysis of 802.11 packets and derive security insights from it!

11:10 AM - 12 PM: The Black Art of Wireless Post-

Exploitation: Bypassing Port-Based Access Controls Using Indirect Wireless Pivots

Gabriel Ryan, Security Engineer at Gotham Digital Science (@s0lst1c3)

Most forms of WPA2-EAP have been broken for nearly a decade. EAP-TTLS and EAP-PEAP have long been susceptible to evil twin attacks, yet most enterprise organizations still rely on these technologies to secure their wireless infrastructure. The reason for this is that the secure alternative, EAP-TLS, is notoriously arduous to implement. To compensate for the weak perimeter security provided by EAP-TTLS and EAP-PEAP, many organizations use port based NAC appliances to prevent attackers from pivoting further into the network after the wireless has been breached. This solution is thought to provide an acceptable balance between security and accessibility. The problem with this approach is that it assumes that EAP is exclusively a perimeter defense mechanism.

In this presentation, we will present a novel type of rogue access point attack that can be used to bypass port-based access control mechanisms in wireless networks. In doing so, we will challenge the assumption that reactive approaches to wireless security are an acceptable alternative to strong physical layer protections such as WPA2-EAP using EAP-TLS.

12:10 - 1 PM: Fortune 100 InfoSec on a State Government Budget

Eric Capuano, SOC Manager at Texas Department of Public Safety (@eric_capuano)

A common misconception is that it takes spending millions to be good at security. Not only is this untrue, but I will share ways that you can increase security posture while actually reducing spending. This talk outlines many of the tricks and mindsets to doing security well without breaking the bank. This is not the typical “Problem, problem, problem...” talk.... This is a solution-based talk that goes back to many of the basic challenges facing SOC teams everywhere.

1:10 - 2 PM: YALDA – Large Scale Data Mining for Threat Intelligence

Gita Ziabari, Senior Threat Research Engineer at Fidelis Cybersecurity (@gitaziabari)

Every SOC is deluged by massive amounts of logs, suspect files, alerts and data that make it impossible to respond to everything. It is essential to find the signal in the noise to be able to best protect an organization. This talk will cover techniques to automate the processing of data mining malware to derive key indicators to find active threats against an enterprise. Techniques will be discussed covering how to tune the automation to avoid false positives and the many struggles we have had in creating appropriate whitelists. We’ll also discuss techniques for organizations to find and process intelligence for attacks targeting them specifically that no vendor can sell or provide them. Audiences would also learn about method of automatically identifying malicious data submitted to a malware analysis sandbox.

2:10 - 3 PM: Past, Present and Future of High Speed Packet Filtering on Linux

Gilberto Bertin, Cloudflare (@jibi42)

As internet DDoS attacks get bigger and more elaborate, the importance of high performance network traffic filtering increases. Attacks of hundreds of millions of packets per second are now commonplace. Unfortunately line rate filtering is still an open problem.

In this session, we will introduce modern techniques for high speed network packet filtering on Linux. We will follow the evolution of the subject, starting with Iptables and userspace offload solutions (such as EF_VI and Netmap), discussing their use cases and their limitations.

We will then move on to a new technology recently introduced

in the Linux kernel called XDP (express data path), which works by hooking an eBPF program into the lowest possible layer in the Linux kernel network stack, allowing network traffic to be filtered at high speeds. We will discuss the strengths of this solution, show some sample XDP programs and give operational tips.

3:10 - 4 PM: Modern Day CovertTCP with a Twist
Mike Raggo, CSO at 802 Secure, Inc. (@MikeRaggo)
Chet Hosmer, Owner of python-forensics.org (@ChetHosmer)

Taking a modern day look on the 20 year anniversary of Craig Rowland's article on Covert TCP, we explore current day methods of covert communications and demonstrate that we are not much better off at stopping these exploits as we were 20 years ago. With the explosion of networked devices using a plethora of new wired and wireless protocols, the covert communication exploit surface is paving new paths for covert data exfiltration and secret communications. In this session, we will explore uPnP, Zigbee, WiFi, P25, Streaming Audio Services, IoT, and much more. Through realworld examples, sample code, and demos; we bring to light this hidden world of concealed communications.

4:10 - 5 PM: Fooling the Hound: Deceiving Domain Admin Hunters
Tom Sela, Head of Security Research at illusive networks

The conflict between cyber attackers and defenders is too often in favor of attackers. Recent results of graph theory research incorporated into red-team tools such as BloodHound, shift the balance even more dramatically towards attackers. Any regular domain user can map an entire network and extract the precise path of lateral movements needed to obtain domain admin credentials or a foothold at any other high-value asset.

In this talk, we present a new practical defensive approach: deceive the attackers. Since the time of Sun Tzu, deceptions have been used on the battlefield to win wars. In recent years, the ancient military tactic of deceptions has been adopted by the cyber-security community in the form of HoneyTokens. Cyber deceptions, such as fictitious high-privilege credentials, are used as bait to lure the attackers into a trap where they can be detected. To shift the odds back in favor of the defenders, the same BloodHound graphs that are generated by attackers should be used by defenders to determine where and how to place bait with maximum effectiveness. In this way, we ensure that any shortest path to a high-value asset will include at least one deceptive node or edge.

5:10 - 6 PM: Hunting Down the Domain Admin and Rob Your Network

Keith Lee, Senior Security Consultant at Trustwave SpiderLabs (@keith55)
Michael Gianarakis, Director of Trustwave SpiderLabs Asia-Pacific

Portia: it's a new tool we have written at SpiderLabs to aid in internal penetration testing engagements. The tool allows you to supply a username and password that you have captured and cracked from Responder or other sources as well as an IP ranges, subnet or list of IP addresses. The tool finds its way around the network and attempts to gain access into the hosts, finds and dumps the passwords/hashes, reuses them to compromise other hosts in the network. In short, the tool helps with lateral movements in the network and automating privilege escalation as well as find sensitive data residing in the hosts.

6:10 - 7 PM: Passwords on a Phone

Sam Bowne (@sambowne)

Almost all Android apps from major retailers store your password on the phone, which is dangerous and unnecessary. And they don't even use the Android KeyStore; they just use custom encryption schemes that generate a key in predictable ways, so passwords are easily recoverable. This is "fake encryption" – the data appears to be encrypted but in fact is not actually protected from attackers. I will present results of my tests of many top retailers, and demonstrate how to steal passwords from them. I will also list a few (very few) companies who actually protect their customers' passwords properly.

Sunday, July 30th

11:10 AM - 12 PM: Demystifying the OPM breach, WTF really happened

Ron Taylor (@Gu5G0rman)

In September 2016 the House Committee on oversight finally released their report. Four years after the original breach, we are still asking how the f*#! did this happen. This talk will go over the key findings of the report and the impact on those who were effected.

12:10 - 1 PM: Go Beyond Tabletop Scenarios by Building an Incident Response Simulation Platform
Eric Capuano, SOC Manager at Texas Department of Public Safety (@eric_capuano)

How prepared is your incident response team for a worst case scenario? Waiting for a crisis to happen before training for a crisis is a losing approach. For things that must become muscle memory, instinctive, you must simulate the event and go through the motions. This talk is a deep-dive technical discussion on how you can build your own DFIR simulation. Best part -- almost all of this can be accomplished with open source tools and inexpensive equipment, but I'll also share tips and tricks on getting free commercial hardware and software for use in your new simulation environment!



MOVIE NIGHT

Join us for thoughtfully curated hacker movies Thursday, Friday and Saturday in Track 4 starting at 20:30.

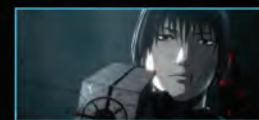
THURSDAY ANIME NIGHT

Ghost in the Shell The New Movie



2015 Set after the events of Arise, the film involves the assassination of the Prime Minister of Japan which is publicly described as the "greatest event since the war". It is up to Public Security Section 9, led by Major Motoko Kusanagi, to discover the true nature of the murder.

Blame!



2017 In the distant technological future, civilization has reached its ultimate Net-based form. An "infection" in the past caused the automated systems to spiral out of order, resulting in a multi-leveled city structure that replicates itself infinitely in all directions. Now humanity has lost access to the city's controls, and is hunted down and purged by the defense system known as the Safeguard.

FRIDAY TOO MANY SECRETS

Sneakers w/special guest John Strauchs



1992 A security pro finds his past coming back to haunt him, when he and his unique team are tasked with retrieving a particularly important item. Join us to help celebrate 25th birthday of DEF CON and Sneakers. Red Team security legend and technical advisor John Strauchs will be in attendance and will participate in a panel discussion and audience questions session immediately after the screening.

iVoted?



2016 'I Voted?' is a feature length, non-partisan documentary which examines the capture and counting of ballots in our elections. It asks the question, "What are the specific assurances of accuracy and security in American voting?", "How do you know your vote counts?", the answers are both surprising and disturbing.

Official Selection: Tribeca 2016
Writer & Director: Jason Grant Smith
Executive Producer: Katie Couric
<http://www.ivotedmovie.com/>

SATURDAY F\$CK THE SYSTEM

Hacking Democracy w/director Russell Michaels hosting a post-film Q&A



2006 The film the voting machine corporations don't want you to see. HACKING DEMOCRACY follows investigator/grandmother, Bev Harris, and her citizen-activists as they set out to uncover how America counts its votes.

Hackers



1995 Cult movie, and the first ever web site to ever be defaced. A young boy is arrested by the US Secret Service for writing a computer virus and is banned from using a computer until his 18th birthday. Years later, he and his friends discover a plot to unleash a dangerous virus. They must use their computer skills to find the evidence while being pursued by the Secret Service and the evil computer genius behind the virus.

CONTESTS

BE THE MATCH



Be part of the coolest bio-hack around - visit the "Be the Match" booth and register for the National Bone Marrow Donor Registry, which helps thousands every year. This will be the seventh year Be the Match has been at DEF CON so swing by, find out more, and even meet members of the DEF CON community that has actually donated marrow and stem cells to those in need!

Where: Contest Area on the forums/pool level.

BEVERAGE COOLING CONTRAFTION CONTEST



Today, you will get the truth. Our beverage is warm. We don't even know what cold beverage is anymore. We need to straighten it out. Those people, you know, they are not sending us their cold beverage. They're not sending their best. They're sending beverages that have lots of problems. They're bringing warm beverages.

We have some warm cervezas here and we need to cool them down.

They left it outside. Can you believe this? It's terrible. It's terrible. And that's what's happening. And it's going to get worse. The organizers, they are not smart people. But I know you people are. You are wonderful beautiful people. Believe me, folks. Believe me. We are going to do very well, very, very well. We are going to build a great chiller. You know that. It's going to be a serious chiller. It's going to be a real chiller. And we are going to make the beverage cold again!

And now for an important public announcement. Once again the BCCC returns to DEFCON! Come out for the science, stay for the beverage. Didn't bring a contraption? Build one and enter the hacked category. You may even win something! Who knows, it could be cool.

Friday 1000 - 1400

BOMB DEFUSE

Remotely navigate an all-terrain robot on a battlefield, and control the robot to defuse a bomb.

Friday, Saturday 1000 - 2000 Sunday 1000 - 1200

CMD+CTRL



We're back! Security Innovation and Women in Security and Privacy are teaming up to bring you two new vulnerable websites that participants will be competing to find vulnerabilities in. All (most) of the vulnerabilities are automatically detected and award points when they're exploited. The sites contain over 100 vulnerabilities including XSS, SQLi, password cracking and more. We'll have easy vulns for beginners as well as more difficult challenges to stump experienced hackers.

Last year was our first year, and we had over 50 people participate. Participants ranged from full-time pentesters to people who wanted to learn what SQL injection was. We've got some handy reference material to help get beginners started.

You will need a laptop to participate, as well as any tools you think you'll need.

Friday, Saturday 1000 - 1800

COINDROIDS



The year is 20X5 and humanity has fallen: now there are only Coindroids. The machines we designed to manage our finances have supplanted and destroyed the human race by turning our own economy against us. Now they battle each other in the ruins of our fallen cities, driven by a single directive: money is power.

Battle your way to the top of the leaderboard by attacking rival droids, or assemble your hacker-fam and compete in the quest to infiltrate Imperial One.

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

Friday, Saturday 1000 - 1800 Sunday 1000 - 1200

CRASH AND COMPILE



What happens when you take an ACM style programming contest, smash it head long into a drinking game, throw in a mix of our most distracting helpers, then shove the resulting chaos incarnate onto a stage? You get the contest known as Crash and Compile.

AND EVENTS

Do you think you can code? Do you think you can code while drinking? We are looking for nine teams who think they have the smarts, the concentration, and the liver to hold up to our gauntlet of programming. Teams who can not only code, but do so with style. We set you against the clock and the other teams. And because they think watching people simply code is boring, our "Team Distraction" is has taken it upon themselves to be creative in hindering you from programming, much to the enjoyment of the audience.

Qualifications take place Friday afternoon in the contest area. Teams of one or two people. Be ready to code, as this won't be easy. The top nine teams who showed themselves ostentatious enough to take on our challenge will compete on the Contest Stage Saturday.

Qualifying: Friday 1100 - 1500

Main Event: Saturday - 1600 - 2000

CYCLEOVERRIDE DEF CON BIKERIDE



Get out your hacker spandex! The 7th annual DEF CON bike ride is here! Every year we get up on Friday of DEF CON and meet outside Caesar's at 5:30am head to a local bike shop and the ride out to Red Rock. We will be doing this Friday AM of DEF CON this year. Be warned - this is a ride at 6am, of DEF CON, in the desert. :x Full info here: www.cycleoverride.org. If you are reading this at DEF CON 25, your best bet is to send us a DM on twitter @cycle_override if you need more info or have questions.

DEF CON BEARD AND MOUSTACHE CONTEST



Held every year since DEF CON 19 in 2011, the DEF CON Beard and Moustache Contest highlights the intersection of facial hair and hacker culture.

For 2017 we will again have three categories:

Full beard: Self-explanatory, for the truly bearded.

Partial Beard or Moustache Only: For those sporting Van Dykes, Goatees, Mutton Chops, and other partial beard styles, as well as moustache only, even if bearded. Bring your Handlebars, Fu Manchus, or whatever adorns your upper lip.

Freestyle: Anything goes, including fake and creatively adorned beards. Creative women often do well in the Freestyle category.

Our esteemed panel of judges determine scores based on presentation, style, whim, and bribery.

Friday, Saturday 1000 - 1800 Sunday 1000 - 1200

DEF CON DARKNET



Our mission is to secure a safe, independent and self-sustaining community free from intrusion and infiltration by those who would enslave us to their own ends. Our adversaries are many and they grow ever more sophisticated - spying

on us through our information streams and controlling us through the messages we are subjected to wherever we go. We must resist. If you join us, you will be sent on quests to improve your current technical knowledge. You'll meet others like you and will learn from each other and grow stronger. Hidden messages you would never have noticed and accomplishments you would never have achieved alone will be yours to discover. You know that you have what it takes to join us. You'll rise through the ranks as you go and get your chance to take on the man running the show by using all of the knowledge that you have acquired.

Friday, Saturday 1000 - 2000 Sunday 1000 - 1200

DEF CON SCAVENGER HUNT

From way back when con was held at the Plaza Hotel & Casino at Defcon 6, through all the years at the Alexis Park, Riviera, Rio, Paris/Bally's, and now Caesars, the Scav Hunt has been doing it's part to make and keep DEF CON weird. Now we're back again to celebrate our twentieth anniversary for three days of dignity selling and debauchery. So come on down to the contest area and find out why year after year people say that the Scavenger hunt is one of the best ways to spend your DEF CON.

Friday, Saturday 1000 - 2000 Sunday 1000 - 1200

DEF CON SHORT STORY CONTEST

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

Originally begun by Nikita, it was then bequeathed to Eris and now Princess Leah and FrozenFOXX are slowly taking over the reins. All stories, regardless of placement, are included in the DEF CON Media Server for DEF CON 25 Materials. Rules, stories and polls are posted on the forums.defcon.org each year!

Winners will be announced on the forums: <https://forum.defcon.org>

CONTESTS

First place receives (2) Human badges, Second place receives (1) Human badge, and by People's Choice poll, one author receives (1) Human badge as well!

DRUNK HACKER HISTORY



The contest that isn't back at DEF CON 25!

The first year proved to the planet that in the game of glittery nostalgic recall, there are no losers and those who won, lost. Last year, we started the creepy clown craze with a single honk of a horn and learn that pop rocks mix with basically anything.

As you know, the DEF CON community has a fluid history of C2H6O consumption. It is a history filled with mephitic adventures, quarter-truths, poor life choices and angry hotel staff. This year, we will, again, scrape the interesting dried stuff off some of the most celebrated, exaggerated moments in Hacker History through the interpretation of a group of pre-selected infamous participants.

Hosted by c7five with judging by jaku - If you like 80s candy, ham sandwiches, lederhosen, lawyer mixology and have nothing better going on, you won't want to miss the third incarnation of Drunk Hacker History!!!

Presented in front of a live DEF CON studio audience with .../.../...

Saturday 2200 - 2359 in Track 2.

FRIENDS OF BILL W. MEETUP

Vegas is a lot of fun, but it can also be just a lot. Too much, even, if you're trying to keep the horizon level in your windscreen. If you're a friend of Bill W joining us for DEF CON 25, please know that we have meetings at noon and five p.m., Thursday through Sunday in "Office 4A", on the promenade level. Drop by if you need to touch base or just want a moment of serenity. We'll be there. (See info booth next to office 4 on the map, if you're having trouble finding "Office 4A")

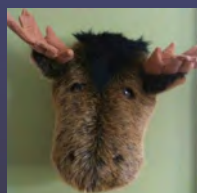
HACKER KARAOKE

Our 9th year! Celebrate with us and with others who love sing. Do you like music? Do you like performances? Want to BE the performer? Want to have that "Hold my beer moment" do your best and not injured? Well trot your happy ass down to Hacker Karaoke, DEFCON's on-site karaoke experience. You can be a star, or if you don't want to be a star, you can also take pride in making an utter fool of yourself.

When: Friday & Saturday - 20:00-02:00

Where: Roman 1, on Promenade Level.

HACK FORTRESS



To the returning competitors, welcome back. For those that have never experienced Hack Fortress, it's a single elimination tournament that runs on Saturday. Thirty minute rounds happen all day Saturday where two teams of TF2 players and hackers battle it out. There's a scoreboard and live spectating

taking place to shame/praise the competitors. So, whether you plan to play or just watch some of the action, stop by and check us out.

If you pre-registered a team, have a team that would like to register or are a standalone looking for a team, stop by anytime on Friday. Round 1 starts Saturday morning at 10:30am. Remember, hackers need a laptop with an ethernet connection, TF2 players need to just show up ready to battle it out.

Friday, Saturday 1000 - 2000 Sunday 1000 - 1200

HAM RADIO LICENSING

Do you know your USB from your LSB? RACES vs ARES? Just don't fret if you can't copy CW because that's no longer on the test. Can you think of a better place to get your ham radio license or upgrade than at DEF CON? Neither can we. Show up with \$15, your ID and FRN, and a copy of your license (if upgrading) and a test slot can be yours. Questions? Come see us! Ready to test? Come see us! The dc408 Ham Exam team can't wait to give you your exclusive DEF CON 25 Ham Radio licensee memento for passing your test at DEF CON. While supplies last, first come first serve.

When: Friday - 1000 - 2000

Where: Capri Room, Promenade Level

INFOSEC UNLOCKED UNIVERSITY: YOUR FIRST TALK

Want to give the next awesome talk in information security? InfoSec Unlocked is a non-profit organization that supports diverse voices at computer security conferences. On Friday, we will be hosting InfoSec Unlocked University where potential new speakers can learn more about entering Call for Papers (CFP) and giving talks at conferences. Attendees will learn from industry veterans about the process of developing talks, submitting to CFPs, creating slides and engaging with audiences during and after the presentation. The rest of the weekend we will host other activities to help connect you with conference organizers, CFP reviewers and fellow future speakers.

<https://isunlocked.com/#/dc25>

Where: Patrician Room on the Forums/Pool level.

When: 11:00 - 19:00

AND EVENTS

MISSION SE IMPOSSIBLE

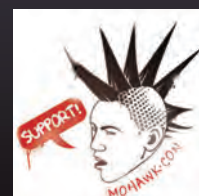


What is Mission SE Impossible (MSI)? Maybe the best way to describe it is if the Gringo Warrior Challenge had a baby with Ethan Hunt while getting some scotch soaked DNA from the Human Hacker, it would give birth to Mission SE Impossible. Also, this baby could shoot lasers out of its eyes.

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

Thursday - All Day in the SE Village

MOHAWK CON



Get your head buzzed at DEF CON to support the Electronic Frontier Foundation, and your favorite hacker charities.

Friday, Saturday, Sunday - 1000-2000

Where: Contest Area on Forums/Pool Level

LAWYER MEETUP

If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join your host Jeff McNamara at 18:00 on Saturday, July 29, for a friendly get-together, followed by dinner/drinks and conversation. Meet in the Consul Boardroom on the Promenade level.

QUEERCON

Queercon Kickoff Thursday 8p to 3a

Mixers: Friday - Sunday, 4p to 6p

QC14 Party - Friday 8p to 3a

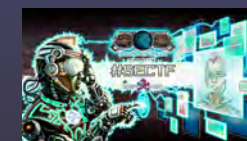
Saturday Dance Party & Queer-Karaoke 8p to 3a

To celebrate 14 years of LGBTQ hacking join Queercon for a weekend of friends and fun. Didn't bring your friends? That's okay, come make new ones. Queercon invites all LGBTQ Defcon attendees, friends and allies to meet and mingle in our open casual environment.

Queercon 14 starts this year with our Kickoff party Thursday night. Friday, Saturday and Sunday we have our Social Mixers at 4pm. Come hang out, meet new people and enjoy our staffed cocktail bar. Don't miss out on the Epic Queercon Party Friday Night starting at 8pm with music from top DJs until 3am. Then on Saturday we have an all-night dance party and Queer-Karaoke starting at 8pm.

Queercon is open to everyone, no Defcon badge required. For the location of all our events including the Queercon Lounge visit queercon.org, our mobile app, Facebook or Twitter.

SECTF



The Social Engineering Capture the Flag, SECTF, returns for its 8th year! Contestants have to fight with their own fears to prove they can SE like the best of them.

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

Friday, Saturday 0930 - 1600 in the SE Village

SECTF4KIDS



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

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

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

Ages 6-12.

All day Friday in the SE Village

SECTF4TEENS



"We have created a series of activities and challenges that will involve things like critical thinking exercises, ciphers, logic puzzles, memory puzzles, verbal and nonverbal challenges, pitting TEENS against TEENS in a test of endurance (and fun).

Ages 13-17.

All day Saturday in the SE Village

SOHOPELESSLY BROKEN

SOHOpelessly
BROKEN

The SOHOpelessly Broken contests, are back at DEF CON 25 in the IoT Village. We have made updates to both tracks and have expanded the CTF

to include a variety of new IoT devices.

CONTESTS

Track 1: One of last year's Black Badge contests is back! 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.

Track 0: The Zero-Day track is focused on the discovery and demonstration of new exploits (0-day vulnerabilities). This track relies on the judging of newly discovered attacks against embedded electronic devices. Devices that are eligible for the contest can be found at iotvillage.org and you can start submitting entries now! The winners who score the highest on their judged entries will be rewarded with cash prizes.

Contestants must provide proof that they disclosed the vulnerability to the vendor in order to be eligible for prizes.

Friday, Saturday 1000 - 1800 Sunday 1000 - 1200

SCHEMAVERSE

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

This unique game gives you direct access to the database that governs the rules. Write SQL queries directly by connecting with any supported PostgreSQL client or use your favourite language to write AI that plays on your behalf. This is DEF CON of course so start working on your SQL injections - anything goes!

Looking to sign up or need a hand? Come visit us at our booth in the Contest Area.

Friday, Saturday 1000 - 1800 Sunday 1000 - 1200

TD FRANCIS X-HOUR FILM CONTEST

@ DEFCON 25 For the fourth year...

This could be the opportunity that's kicking open the door to your film making greatness... Assemble your team of 5 or less (director, producer, writer, camera/ photography, editor) and make your "Crime/Hacker Capers" inspired/ themed cinematic marvel of short film here at DEFCON. Actors and extras don't count towards the max 5, so 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.

Prizes include Human Badges for DEFCON 26, \$5000 scholarships to Seattle Film Institute, VideoMaker Magazine subscriptions, iPitch subscriptions (and other cool TBD stuff).

All completed films will be screened 18:30 Saturday night in Track 4, Octavius ballroom, Promenade South.

Chances to win raffle prizes, give aways, cash bar, and fun, love, applause, laughs, and cheers for all... 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 DEFCON 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 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 things and stuff - not filming in designated no-camera areas - obtaining permission when appropriate - and being approachable and courteous to all.

Cheers, Waz

@DEFCONFilmConte

www.xhourfilmcontest.com

TINFOIL HAT CONTEST



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

"Substance" award for that category. We all know that hacker culture is all about looking good, though, so a single winner will be selected from all submissions for "Style". Finally, a single overall winner will be selected from all combined categories for "Style and Substance". Bonus points will be awarded for wearing your hat around DEF CON.

Friday, Saturday 1000 - 1800 Sunday 1000 - 1200

WARLOCK GAM3Z

warl0ck gam3z

warl0ck gam3z is a hands-on 24/7; throw-down, no-holds-barred hacker competition

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

Most challenges require participants to download something that pertains to the problem at hand and solve the challenge using whatever tools, techniques or methods they have available.

One participant will become the leader of the board and they control which challenges are available. Being the leader of the board is a double edge sword. Regular participants may choose to back out of a challenge if they cannot solve it but once the leader of the board selects a challenge; they must answer/solve it or be passed by a new leader as they are not afforded the same luxury of just backing out. And just to keep it interesting, occasionally "The Judge" challenge comes out and is made available to everyone except the current leader of the board.

Friday, Saturday 1000 - 2000

WHOSE SLIDE IS IT ANYWAY?



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 20 short decks on whatever nonsense tickles our fancy that week. 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 five-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 Demo Gods, it's a night of schadenfreude for the whole family.

The Where: Track 4, Promenade South

The When: Friday & Saturday 20:00 - ??:??

WIRELESS CTF



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

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

Keep an eye on @wctf_us and @WIFI_Village

LINKS: Check out our website for tools, what you need, and what to do. Enjoy your journey.

<http://wirelessvillage.ninja> and <http://sdr.ninja/>

Tools/tips: <http://www.wirelessvillage.ninja/resources.html>

<http://sdr.ninja/training-events/sdr-wctf/>

Introducing the 2017 TDF X-Hour Film Festival!

THURSDAY - Track 4, Octavius ballroom, Promenade South.

When: 018:00 - 20:00

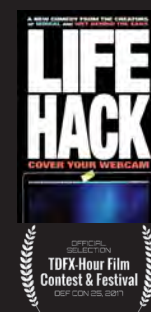
LIFE HACK (2017)

90 minutes + Q&A with Director

Life Hack is an incredibly timely ensemble comedy about digital privacy... or lack thereof. A humorous cautionary tale about cyber threats in the digital age. Cover your webcam.

Director and Writer: Sloan Copeland Producers: Jessica Copeland, Sloan Copeland, Doug Roland, Benjamin Zimbric Cinematographer: Benjamin Zimbric Cast: Devin Ratray, Derek Wilson, Sean Kleier, Jonathan Roomie, Margaret Keane Williams, Christine Cartell

An official 2017 TDF X-Hour Film Festival @ DEF CON Selection, and winner of the 2017 Brooklyn Film Festival best screen play award. Life Hack's director, producers, and some cast and crew will be joining us for this screening and will be available for audience questions immediately following.



FRIDAY - Track 4, Octavius ballroom, Promenade South.

When: 019:00 - 20:00

CYBORGS - SHOULD WE BE BETTER THAN WE ARE? (2017)

18 min. - Documentary

Humans have always used body enhancements, but should we be better than we are? If we want to be a cyborg, at what point, if any, should government be involved?

Director/Writer/Producer: Victoria Sutton



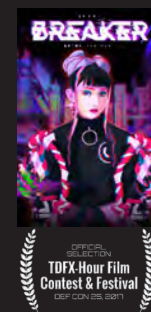
BREAKER - (2017)

11 min - Narrative

In tomorrow's Tokyo, the technologically-enhanced body of a young mercenary hacker is overrun by a sentient data weapon. Wanted, the parasitic A.I becomes her only ally as she is chased across the city by those seeking to salvage it.

Director/Writer/Producer: Philippe McKie Cinematographer: Hans Bobanovits

Sound Editor: Remy Sealey Key Cast: Yuka Tomatsu, Arisa Hanzawa, Kazuya Shimizu



SATURDAY - Track 4, Octavius ballroom, Promenade South.

When: 019:00 - 20:00

SCREENING OF THIS YEAR'S ENTRIES INTO THE TD FRANCIS X-HOUR FILM CONTEST



CAPTURE THE FLAG

DEF CON Capture The Flag is the most intense, most wild, and most hardcore test of hacker skill. The most rockin' bands of hackers on Planet Earth will be blasting binaries, rocking registers, and smashing stacks in an epic three-day event. If you think you've seen it all, you've got another thing comin': this year's game runs on the never-before-seen cLEMENCY computer architecture. Will teams be riding on the wind or screaming for vengeance? You'll just have to find out!

HOW TO COMPETE

DEF CON CTF has limited space for competitors, and teams can be qualified by winning the previous year, placing in previously-approved qualifying competitions online and around the world, or scoring well in our qualification event, held in April this year.

THE CTF ROOM

Want to find out who is stronger, who is amazing, and who will survive in America? Visit the CTF room in the contest area to see it all: the highlights, the low lights, the addiction, and the heartbreak. Watch players analyze binaries, enjoy game visualizations, and check out how your favorite team is doing.

Enjoy yourself, but be respectful and don't interrupt hackers hard at work. If you have questions about CTF, talk with a member of Legitimate Business Syndicate. Competitors may be willing to talk if they're not engrossed in the game too.

THE FINAL COUNTDOWN

Five years is a long time to run a Capture the Flag event. We're leaving together after this year, and while still it's farewell, we can't wait to see what new blood brings to DEF CON CTF in 2018 and beyond.

We would not be able to run a successful competition this last five years without the energy, inventiveness, and skill of the CTF and DEF CON communities. Thanks to all CTF competitors and organizers around the world for welcoming us into the community. We'd like to especially thank the DEF CON organizers and goons for our five years in this exceptional venue.

Most of all, thank you to all DEF CON attendees: you've all made this a special and unforgettable part of our lives, and we can't wait to see what you build and/or break next.

<3 Legitimate Business Syndicate

LINKS

Game Schedule, Scores, Blog
<https://legitbs.net/>

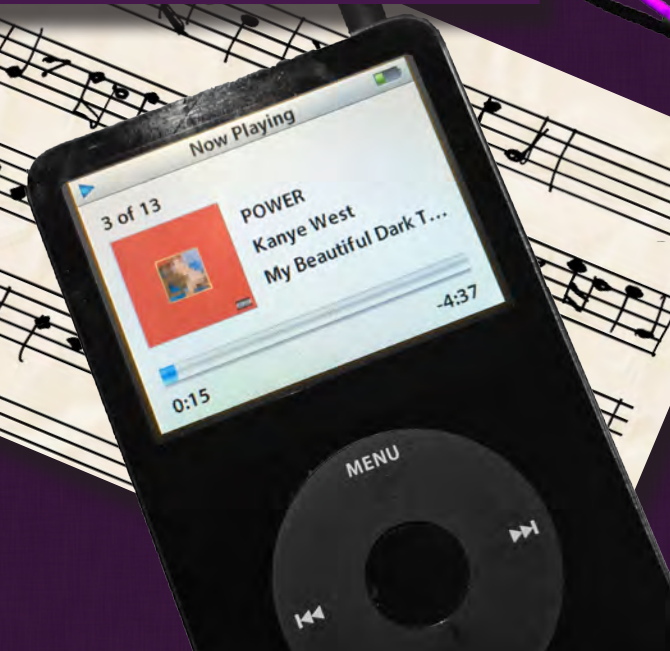
Announcements and News
https://twitter.com/legitbs_ctf

LEGITIMATE BUSINESS SYNDICATE

Deadwood
Fuzyll
Gyno
HJ
Hoju
Jymbolia
Lightning
Selir
Sirgoon
Vito

B9 BA AB B3 FS AF
BA A9 FS B9 AE
FS BC AB BC A1 E9

BD B8 BF FS BS B4
AF B6 BA B7 AC BA
A9 BE FS A9 AE F4
B0 B4 B0 BS AE B6



PRESENTATIONS

Alpha by Speaker

UNTRUSTWORTHY HARDWARE AND HOW TO FIX IT

Sunday at 10:00 in Track 4
20 minutes | Demo, Tool

Octane, Hacker

Modern computing platforms offer more freedom than ever before. The rise of Free and Open Source Software has led to more secure and heavily scrutinized cryptographic solutions. However, below the surface of open source operating systems, strictly closed source firmware along with device driver blobs and closed system

architecture prevent users from examining, understanding, and trusting the systems where they run their private computations. Embedded technologies like Intel Management Engine pose significant threats when, not if, they get exploited. Advanced attackers in possession of firmware signing keys, and even potential access to chip fabrication, could wreak untold havoc on cryptographic devices we rely on.

After surveying all-too-possible low level attacks on critical systems, we will introduce an alternative open source solution to peace-of-mind cryptography and private computing. By using programmable logic

chips, called Field Programmable Gate Arrays, this device is more open source than any common personal computing system to date. No blobs, no hidden firmware features, and no secret closed source processors. This concept isn't "unhackable", rather we believe it to be the most fixable; this is what users and hackers should ultimately be fighting for.

EVADING NEXT-GEN AV USING ARTIFICIAL INTELLIGENCE

Saturday at 11:00 in Track 4
20 minutes | Demo

Hyrum Anderson, Technical Director
of Data Science, Endgame

Much of next-gen AV relies on machine learning to generalize to never-before-seen malware. Less well appreciated, however, is that machine learning can be susceptible to attack by, ironically, other machine learning models. In this talk, we demonstrate an AI agent trained through reinforcement learning to modify malware to evade machine learning malware detection. Reinforcement learning has produced game-changing AI's that top human level performance in the game of Go and a myriad of hacked retro Atari games (e.g., Pong). In an analogous fashion, we demonstrate an AI agent that has learned through thousands of "games" against a next-gen AV malware detector which sequence of functionality-preserving changes to perform on a Windows PE malware file so that it bypasses the detector. No math or machine learning background is required; fundamental understanding of malware and Windows PE files is a welcome; and previous experience hacking Atari Pong is a plus.

DEALING THE PERFECT HAND - SHUFFLING MEMORY BLOCKS ON Z/OS

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

Ayou13, Pentester, Wavestone

Follow me on a journey where we p0wn one of the most secure platforms on earth. A giant mammoth that still powers the most critical business functions around the world: The Mainframe! Be it a wire transfer, an ATM withdrawal, or a flight booking, you can be sure that you've used the trusted services of a Mainframe at least once during the last 24 hours. In this talk, I will present methods of privilege escalation on IBM z/OS: How to leverage a simple access to achieve total control over the machine and impersonate other users. If you are interested in mainframes or merely curious to see a what a shell looks like on MVS, you're welcome to tag along.

BITSINJECT

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

Dor Azouri, Security researcher, @
SafeBreach

Windows' BITS service is a middleman for your download jobs. You start a BITS job, and from that point on, BITS is responsible for the download. But what if we tell you that BITS is a careless middleman? We have uncovered the way BITS maintains its jobs queue using a state file on disk, and found a way for a local administrator to control jobs using special modifications to that file.

Comprehending this file's binary structure allowed us to change a job's properties (such as RemoteURL, Destination Path...) in runtime and even inject our own custom job, using none of BITS' public interfaces. This method, combined with the generous notification feature of BITS, allowed us to run a program of our will as the LocalSystem account, within session 0. So if you wish to execute your code as NT AUTHORITY/SYSTEM and the first options that come to mind are psexec/creating a service, we now add a new option: BITSInject.

Here, we will not only introduce the practical method we formed, but also: Reveal the binary structure of the state file for you to play with, and some knowledge we gathered while researching the service flow

We will also provide free giveaways: A one-click python tool that performs the described method; SimpleBITSServer - a pythonic BITS server; A struct definition file, to use for parsing your BITS state file

UNBOXING ANDROID: EVERYTHING YOU WANTED TO KNOW ABOUT ANDROID PACKERS

Sunday at 10:00 in 101 Track
45 minutes | Demo, Tool

Avi Bashan, Mobile R&D Team
Leader, Check Point

Slava Makkaveev, Security
Researcher, Check Point

To understand the Android ecosystem today, one must understand Android packers. Whether used for protecting legitimate apps' business logic or hiding malicious content, Android packer

usage is on the rise. Android packers continue to increase their efforts to prevent reverse engineers and static analysis engines from understanding what's inside the package. To do so they employ elaborate tactics, including state of the art ELF tampering, obfuscation and various anti-debugging techniques.

In this talk, we will provide an overview of the packer industry and present real world test cases. We will do a deep technical dive into the internal workings of popular Android packers, exposing the different methods which protect the app's code. As a countermeasure, we will provide various techniques to circumvent them, allowing hackers and security researchers to unpack the secrets they withhold.

MICROSERVICES AND FAAS FOR OFFENSIVE SECURITY

Saturday at 11:00 in 101 Track
20 minutes | Demo

Ryan Baxendale

There are more cloud service providers offering serverless or Function-as-a-service platforms for quickly deploying and scaling applications without the need for dedicated server instances and the overhead of system administration. This technical talk will cover the basic concepts of microservices and FaaS, and how to use them to scale time consuming offensive security testing tasks. Attacks that were previously considered impractical due to time and resource constraints can now be considered feasible with the availability of cloud services and the never-ending free flow of public IP addresses to avoid attribution and blacklists.

Key takeaways include a guide to scaling your tools and a demonstration on the practical benefits of utilising cloud services in performing undetected port scans, opportunistic attacks against short lived network services, brute-force attacks on services and OTP values, and creating your own whois database, shodan/censys, and searching for the elusive internet accessible IPv6 hosts.

PRESENTATIONS

**HACKER
JEOPARDY**
LIVE FROM THE VOMITORILUM!

TRACTUS II
VENERIS ET SATURNI
XX HORIS

DFIV

XVIII+ ONLY

FRI-SAT 8PM, IDIOT

PRESENTATIONS

JAILBREAKING APPLE WATCH

Thursday at 12:00 in 101 Track 2
45 minutes | Demo

Max Bazaliy, Security Researcher, Lookout

On April 24, 2015, Apple launched themselves into the wearables category with the introduction of Apple Watch. This June, at Apple's Worldwide Developer Conference, Apple announced that their watch is not only the #1 selling smartwatch worldwide by far, but also announced the introduction of new capabilities that will come with the release of watchOS 4. Like other devices, Apple Watch contains highly sensitive user data such as email and text messages, contacts, GPS and more, and like other devices and operating systems, has become a target for malicious activity.

This talk will provide an overview of Apple Watch and watchOS security mechanisms including codesign enforcement, sandboxing, memory protections and more. We will cover vulnerabilities and exploitation details and dive into the techniques used in creating an Apple Watch jailbreak. This will ultimately lead to a demonstration and explanation of jailbreaking an Apple Watch, showcasing how it can access important user data and applications.

STARTING THE AVALANCHE: APPLICATION DDoS IN MICROSERVICE ARCHITECTURES

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

Scott Behrens, Senior Application Security Engineer

Jeremy Heffner, Senior Cloud Security Engineer

We'd like to introduce you to one of the most devastating ways to cause service instability in modern micro-service architectures: application DDoS. Unlike traditional network DDoS that focuses on network pipes and edge resources, our talk focuses on identifying and targeting expensive calls within a micro-services architecture, using their complex interconnected relationships to cause the system to attack itself — with massive effect. In modern microservice architectures it's easier

to cause service instability with sophisticated requests that model legitimate traffic to pass right through web application firewalls.

We will discuss how the Netflix application security team identified areas of our microservices that laid the groundwork for these exponential-work attacks. We'll step through one case study of how a single request into an API endpoint fans out through the application fabric and results in an exponential set of dependent service calls. Disrupting even one point within the dependency graph can have a cascading effect throughout not only the initial endpoint, but the dependent services backing other related API services.

We will then discuss the frameworks we collaborated on building that refine the automation and reproducibility of testing the endpoints, which we've already successfully leveraged against our live production environment. We will provide a demonstration of the frameworks which will be open sourced in conjunction with this presentation. Attendees will leave this talk understanding architectural and technical approaches to identify and remediate application DDoS vulnerabilities within their own applications. Attendees will also gain a greater understanding on how to take a novel new attack methodology and build an orchestration framework that can be used at a global scale.

THE CALL IS COMING FROM INSIDE THE HOUSE! ARE YOU READY FOR THE NEXT EVOLUTION IN DDoS ATTACKS?

Sunday at 12:00 in Track 3
45 minutes | Art of Defense

Steinthor Bjarnason, Senior Network Security Analyst, Arbor Networks

Jason Jones, Security Architect, Arbor Networks

The second half of 2016 saw the rise of a new generation of IoT botnets consisting of webcams and other IoT devices. These botnets were then subsequently used to launch DDoS attacks on an unprecedented scale against Olympic-affiliated organizations, OVH, the web site of Brian Krebs and Dyn.

Early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters, vastly exceeds those directly accessible from the Internet, allowing for the creation of botnets with unprecedented reach and scale.

This reveals an evolution in the threat landscape that most organizations are completely unprepared to deal with and will require a fundamental shift in how we defend against DDoS attacks.

This presentation will include:- An analysis of the Windows Mirai seeder including its design, history, infection vectors and potential evolution.- The DDoS capabilities of typically infected IoT devices including malicious traffic analysis.- The consequences of infected IoT devices inside the corporate network including the impact of DDoS attacks, originating from the inside, targeting corporate assets and external resources.- How to detect, classify and mitigate this new threat.

ABUSING CERTIFICATE TRANSPARENCY LOGS

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

Hanno Böck, Hacker and freelance journalist

The Certificate Transparency system provides public logs of TLS certificates. While Certificate Transparency is primarily used to uncover security issues in certificates, its data is also valuable for other use cases. The talk will present a novel way of exploiting common web applications like Wordpress, Joomla or Typo3 with the help of Certificate Transparency.

Certificate Transparency has helped uncover various incidents in the past where certificate authorities have violated rules. It is probably one of the most important security improvements that has ever happened in the certificate authority ecosystem. In September 2017 Google will make Certificate Transparency mandatory for all new certificates. So it's a good time to see how it could be abused by the bad guys.

REVOKE-OBUSCATION: POWERSHELL OBFUSCATION DETECTION (AND EVASION) USING SCIENCE

Sunday at 13:00 in Track 4
45 minutes | Art of Defense, Demo, Tool

Daniel Bohannon (DB0), Senior Consultant, MANDIANT

Lee Holmes, Lead Security Architect, Microsoft

Attackers, administrators and many legitimate products rely on PowerShell for their core functionality. However, its power has made it increasingly attractive for attackers and commodity malware authors alike. How do you separate the good from the bad?

A/V signatures applied to command line arguments work sometimes. AMSI-based (Anti-malware Scan Interface) detection performs significantly better. But obfuscation and evasion techniques like Invoke-Obfuscation can and do bypass both approaches.

Revoke-Obfuscation is a framework that transforms evasion into a treacherous deceit. By applying a suite of unique statistical analysis techniques against PowerShell scripts and their structures, what was once a cloak of invisibility is now a spotlight. It works with .vtx files, command lines, scripts, ScriptBlock logs, Module logs, and is easy to extend.

Approaches for evading these detection techniques will be discussed and demonstrated.

Revoke-Obfuscation has been used in numerous Mandiant investigations to successfully identify obfuscated and non-obfuscated malicious PowerShell scripts and commands. It also detects all obfuscation techniques in Invoke-Obfuscation, including two new techniques being released with this presentation.

GAME OF DRONES: PUTTING THE EMERGING 'DRONE DEFENSE' MARKET TO THE TEST

Saturday at 16:00 in Track 4
45 minutes | Art of Defense, Demo, Tool

Francis Brown, Partner, Bishop Fox

David Latimer, Security Analyst, Bishop Fox

When you learned that military and law enforcement agencies had trained screaming eagles to pluck drones from the sky, did you too find yourself asking: "I wonder if I could throw these eagles off my tail, maybe by deploying delicious bacon countermeasures?" Well you'd be wise to question just how effective these emerging, first generation "drone defense" solutions really are, and which amount to little more than "snake oil".

There is no such thing as "best practices" when it comes to defending against "rogue drones", period. Over the past 2 years, new defensive products that detect and respond to "rogue drones" have been crawling out of the woodwork. The vast majority are immature, unproven solutions that require a proper vetting.

We've taken a MythBusters-style approach to testing the effectiveness of a variety of drone defense solutions, pitting them against our DangerDrone. Videos demonstrating the results should be almost as fun for you to watch as they were for us to produce. Expect to witness epic aerial battles against an assortment of drone defense types, including:

- trained eagles and falcons that hunt "rogue drones"
- fighter drones that hunt and shoot nets
- drones with large nets that swoop in and snatch up "rogue drones"
- surface-to-air projectile weapons, including bazooka-like cannons that launch nets, and shotgun shells containing nets
- signal jamming and hijacking devices that attack drone command and control interfaces
- even frickin' laser beams and Patriot missiles!

We'll also be releasing DangerDrone v2.0, an upgraded version of our free Raspberry Pi-based pentesting quadcopter (basically a ~\$500 hacker's laptop, that can also fly). We'll be giving away a fully functional DangerDrone v2.0 to one lucky audience member! So come see what's guaranteed to be the most entertaining talk this year and find out which of these dogs can hunt!

HOW WE CREATED THE FIRST SHA-1 COLLISION AND WHAT IT MEANS FOR HASH SECURITY

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

Elie Bursztein, Anti-abuse research lead, Google

In February 2017, we announced the first SHA-1 collision. This collision combined with a clever use of the PDF format allows attackers to forge PDF pairs that have identical SHA-1 hashes and yet display different content. This attack is the result of over two years of intense research. It took 6500 CPU years and 110 GPU years of computations which is still 100,000 times faster than a brute-force attack.

In this talk, we recount how we found the first SHA-1 collision. We delve into the challenges we faced from developing a meaningful payload, to scaling the computation to that massive scale, to solving unexpected cryptanalytic challenges that occurred during this endeavor.

We discuss the aftermath of the release including the positive changes it brought and its unforeseen consequences. For example it was discovered that SVN is vulnerable to SHA-1 collision attacks only after the WebKit SVN repository was brought down by the commit of a unit-test aimed at verifying that Webkit is immune to collision attacks.

Building on the Github and Gmail examples we explain how to use counter-cryptanalysis to mitigate the risk of a collision attacks against software that has yet to move away from SHA-1. Finally we look at the next generation of hash functions and what the future of hash security holds

PRESENTATIONS

XENOSCAN: SCANNING MEMORY LIKE A BOSS

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

Nick Cano, Hacker

XenoScan is the next generation in tooling for hardcore game hackers. Building on the solid foundation from older tools like Cheat Engine and Tsearch, XenoScan makes many innovations which take memory scanning to a whole new level.

This demo-heavy talk will skip the fluff and show the power of the tool in real-time. The talk will demonstrate how the tool can scan for partial structures, detect complex data structures such as binary trees or linked lists, detect class-instances living on the heap, and even group detected class instances by their types. Additional, these demos will take a look at the tool's extensibility by working not only on native processes, but also on Nintendo games running in emulators. You're not all game hackers, so the talk will also show how XenoScan can be useful in the day-to-day workflow of reverse engineers and hackers.

When I'm not doing demos, I'll be drilling down to the low-level to talk about the nitty gritty details of what's happening, how it works, and why it works.

By the end of the talk, you'll see the true power of a well-made, smart memory scanner. You'll be empowered to use it in your day to day hacking, whether that is on games, malware, or otherwise. For those of you that are really interested in the tool, it is completely open-source and all development is done on an interactive livestream, meaning you can participate in and learn from future development.

WEAPONIZING THE BBC MICRO:BIT

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

Damien "virtualabs" Cauquil,
Senior security researcher,
Econocom Digital Security

In 2015, BBC sponsored Micro:Bit was launched and offered to one million students in the United Kingdom to teach them how to code. This device is affordable and have a lot of features and can be programmed in Python rather than C++ like the Arduino. When we discovered

this initiative in 2016, we quickly thought it was possible to turn this tiny device into some kind of super-duper portable wireless attack tool, as it is based on a well-known 2.4GHz RF chip produced by Nordic Semiconductor.

It took us a few months to hack into the Micro:Bit firmware and turn it into a powerful attack tool able to sniff keystrokes from wireless keyboards or to hijack and take complete control of quadcopters during flight. We also developed many tools allowing security researchers to interact with proprietary 2.4GHz protocols, such as an improved sniffer inspired by the mousejack tools designed by Bastille. We will release the source code of our firmware and related tools during the conference.

The Micro:Bit will become a nifty platform to create portable RF attack tools and ease the life of security researchers dealing with 2.4GHz protocols!

GHOST IN THE DROID: POSSESSING ANDROID APPLICATIONS WITH PARASPECTRE

Sunday at 10:20 in Track 4
20 minutes | Demo, Tool

chaosdata, Senior Security
Consultant, NCC Group

Modern Android applications are large and complex, and can be a pain to analyze even without obfuscation - static analysis can only get one so far, the debugger sucks, Frida doesn't give you enough access to the Java environment, and editing smali or writing Xposed hooks can be time consuming and error prone. There has to be a better way!

What if we could inject a command line REPL into an app to drive functionality? And what if we could also make writing function hooks fast and easy?

In this talk, I will introduce ParaSpectre, a platform for dynamic analysis of Android applications that injects JRuby into Android applications. It bundles a hook configuration web API, a web application interface to configure and edit hooks, and a connect-back JRuby REPL to aid application exploration from the inside-out. It supports various selectors to match classes and

methods, can be reconfigured on-the-fly without requiring a device reboot, and takes the pain out of writing method hooks for Android apps.

ParaSpectre is for developers and security researchers alike. While not itself a debugger, it provides a level of access into a running application that a debugger generally won't.

INSIDE THE 'MEET DESAI' ATTACK: DEFENDING DISTRIBUTED TARGETS FROM DISTRIBUTED ATTACKS

Thursday at 15:00 in 101 Track
45 minutes | Art of Defense

CINCVo1FLT (Trey Forgety), Director
of Government Affairs & IT Ninja,
NENA: The 9-1-1 Association

In October of 2016, a teenage hacker triggered DDoS attacks against 9-1-1 centers across the United States with five lines of code and a tweet. This talk provides an in-depth look at the attack, and reviews and critiques the latest academic works on DDoS attacks directed at 9-1-1 systems. It then discusses potential mitigation strategies for legacy TDM and future all-IP access networks, as well as disaggregated "over-the-top" originating services and the devices on which both the access network providers and originating service providers rely.

WSUSPENDU: HOW TO HANG WSUS CLIENTS

Saturday at 10:20 in Track 3h
20 minutes | Demo, Tool

Romain Coltel, Lead product
manager at Alsid

Yves Le Provost, Security auditor
at ANSSI

You are performing a pentest. You just owned the first domain controller. That was easy. All the computers are belong to you. But unfortunately, you can't reach the final goal. The last target is further in the network, non accessible and heavily filtered. Thankfully, one last hope remains. You realize the target domain pulls its updates from the WSUS server of the compromised domain, the one you fully control. Hope is back... But once again, it fails. The only tools available for controlling the updates are

not working: they require a network attack that is prevented by the network architecture and the server configuration. All hope is lost...

We will present you a new approach, allowing you to circumvent these limitations and to exploit this situation in order to deliver updates. Thus, you will be able to control the targeted network from the very WSUS server you own. By extension, this approach may serve as a basis for an air gap attack for disconnected networks.

Our talk will describe vulnerable architectures to this approach and also make some in-context demonstration of the attack with new public tooling. Finally, as nothing is inescapable, we will also explain how you can protect your update architecture.

DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

Saturday at 20:00 - 22:00 in Modena
Room
Evening Lounge

Christian "quaddi" Dameff MD MS,
Hacker

Jeff "r3plican" Tully MD, Hacker

Beau Woods, Deputy director of the
Cyber Statecraft Initiative in the
Brent Scowcroft on International
Security

Joshua Corman, Director of the
Cyber Statecraft Initiative at the
Atlantic Council's Brent Scowcroft
Center

Michael C. McNeil, Privacy
and security expert, Philips
Healthcare

Jay Radcliffe, Senior Security
Consultant and Researcher, Rapid7

Suzanne Schwartz, MD, MBA,
Associate Director for Science &
Strategic Partnerships, FDA/Center
for Devices & Radiological Health
(CDRH)

Previously a free-flowing, fast moving conversation between old friends and new colleagues in a dimly lit and alcohol soaked off-strip hotel suite, the third annual edition of "DO No H4rm" moves to the better lit and even more alcohol soaked auspices of the DEF CON 25 Evening Lounge for a two hour session that links makers, breakers, and wonks in the healthcare space for a continuation of what may be one of the most important conversations in

PRESENTATIONS

DEF CON 101 PANEL

Thursday at 16:00 in 101 Track
105 minutes | Hacker History,
Audience Participation

HighWiz, Founder, DC101

Malware Unicorn

Niki7a, Director of Content &
Coordination, DEF CON

Roamer, CFP Vocal Antagonizer, DEF
CON

Wiseacre

Shaggy

The DEF CON panel is the place to go to learn about the many facets of DEF CON and to begin your DEF CONian Adventure. Here you will begin your adventure that will include more than just listening in the talk tracks. You can get hands-on experience in the Villages and witness amazing feats of programming in Demo Labs. You may even display your own powers by participating in a contest or two in the Events and Contest Area. The panel will give you what you need to know to navigate DEF CON to your best advantage. We have speakers who will regale you with tales of how they came to be at DEF CON and (hopefully) inspire you with their personal experiences. Oh yeah, there is the time honored "Name the Noob", with lots of laughs and even some prizes.

PANEL: DEF CON GROUPS

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

Jeff Moss (Dark Tangent), Founder,
DEF CON

Waz, DCG

Brent White (B1TKILL3R), DCG and
DC615

Jayson E. Street, DCG Ambassador

Gripter, DC801

Jun Li, DC010

SDups, DC225

Major Malfunction, DC4420

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 talk, you'll hear from DEF CON's founder, Dark Tangent, who is also moderating the panel. Jayson E. Street, the Ambassador of DEF CON groups will also discuss updates about the program and share information

PRESENTATIONS

from his global travel to help start groups around the world. We will also discuss what DEF CON groups are, how to get involved, as well as ideas for how to run a group, location ideas, and how to spread the word.

Founders of their own local DEF CON groups will also discuss the awesome projects of their groups, as well as projects from other groups, to give ideas to take back to your own DEF CON group. Projects we'll discuss range from custom badge build, IoT devices, vintage gaming systems, custom built routers, smarthome devices and more!

FROM BOX TO BACKDOOR: USING OLD SCHOOL TOOLS AND TECHNIQUES TO DISCOVER BACKDOORS IN MODERN DEVICES

Thursday at 11:00 in 101 Track
45 minutes

Patrick DeSantis, Senior Security Research Engineer, Cisco Talos

Stringing together the exploitation of several seemingly uninteresting vulnerabilities can be a fun challenge for security researchers, penetration testers, and malicious attackers. This talk follows some of the paths and thought processes that one researcher followed while evaluating the security of several new "out of the box" Industrial Control System (ICS) and Internet of Things (IoT) devices, using a variety of well known exploitation and analysis techniques, and eventually finding undocumented, root-level, and sometimes un-removable, backdoor accounts.

KOADIO C3 - WINDOWS COM COMMAND & CONTROL FRAMEWORK

Saturday at 13:00 in Track 2
45 minutes | Demo, Tool

Sean Dillon (zerosum0x0), Senior Security Analyst, RiskSense, Inc.

Zach Harding (Aleph-Naught-), Senior Security Analyst, RiskSense, Inc.

Koadic C3, or COM Command & Control, is a Windows post-exploitation tool similar to other penetration testing rootkits such as Meterpreter and Powershell Empire. The major difference is that Koadic does most of its operations using the Windows Script Host (a.k.a. JScript/VBScript),

with compatibility in the core to support a default installation of Windows 2000 with no service packs (and potentially even versions of NT4) all the way through Windows 10.

An in-depth view of default COM objects will be provided. COM is a fairly underexplored, large attack surface in Windows. We will share lots of weird Windows scripting quirks with interesting workarounds we discovered during the course of development. Post exploitation with PowerShell has grown in popularity in recent years, and seeing what can be done with just the basic Windows Script Host is an interesting exploration. In addition, defenses against this type of tool will be discussed, as the Windows Script Host is more tightly coupled to the core of Windows than PowerShell is.

It is possible to serve payloads completely in memory from stage 0 to beyond, as well as use cryptographically secure communications over SSL and TLS (depending on what the victim OS has available). We also found numerous ways to "fork to shellcode" in an environment which traditionally does not provide such capabilities. This talk is based on original research by ourselves, as well as the previous amazing work of engima0x3, subTee, tiraniddo, and others.

NEXT-GENERATION TOR ONION SERVICES

Friday at 13:00 in Track 4
45 minutes | 0025

Roger Dingledine, The Tor Project

Millions of people around the world use Tor every day to protect themselves from surveillance and censorship. While most people use Tor to reach ordinary websites more safely, a tiny fraction of Tor traffic makes up what overhyped journalists like to call the "dark web". Tor onion services (formerly known as Tor hidden services) let people run Internet services such as websites in a way where both the service and the people reaching it can get stronger security and privacy.

I wrote the original onion service code as a toy example in 2004, and it sure is showing its age. In particular, mistakes in the original protocol are now being actively exploited by fear-mongering "threat intelligence" companies to build lists of onion services even when the service operators thought they would stay under the radar.

These design flaws are a problem because people rely on onion services for many cool use cases, like metadata-free chat and file sharing, safe interaction between journalists and their sources, safe software updates, and more secure ways to reach popular websites like Facebook.

In this talk I'll present our new and improved onion service design, which provides stronger security and better scalability. I'll also publish a new release of the Tor software that lets people use the new design.

\$BIGNUM STEPS FORWARD, \$TRUMFNUM STEPS BACK: HOW CAN WE TELL IF WE'RE WINNING?

Saturday at 10:00 in Track 245
minutes

Cory Doctorow, craphound.com, science fiction author, activist, journalist and blogger.

Is Net Neutrality on the up or down? Is DRM rising or falling? Is crypto being banned, or will it win, and if it does, will its major application be ransomware or revolution? Is the arc of history bending toward justice, or snapping abruptly and plummeting toward barbarism?

It's complicated.

A better world isn't a product, it's a process. The right question isn't, "Does the internet make us better or worse," it's: "HOW DO WE MAKE AN INTERNET THAT MAKES THE WORLD BETTER?" We make the world better with code, sure, but also with conversations, with businesses, with lawsuits and with laws.

We don't know how to get to a better world, but we know which direction it's in, and we know how to hill-climb towards it. If we keep heading that way, we'll get "somewhere". Somewhere good. Somewhere imperfect. Somewhere where improvement is possible.

BREAKING THE X86 INSTRUCTION SET

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

Christopher Dumas, Security Researcher, Battelle Memorial Institute

A processor is not a trusted black box for running code; on the contrary, modern x86 chips are packed full of secret instructions and hardware bugs. In this talk, we'll demonstrate how page fault analysis and some creative processor fuzzing can be used to exhaustively search the x86 instruction set and uncover the secrets buried in your chipset. We'll disclose new x86 hardware glitches, previously unknown machine instructions, ubiquitous software bugs, and flaws in enterprise hypervisors. Best of all, we'll release our sandsifter toolset, so that you can audit - and break - your own processor.

WELCOME TO DEF CON 25

Friday at 10:00 in Track 2
20 minutes | Hacker History

The Dark Tangent, Founder, DEF CON

The Dark Tangent welcomes everyone to DEF CON 25, our silver anniversary!

DARK DATA

Friday at 15:00 in Track 3
45 minutes

Svea Eckert, NDR

Andreas Dewes, PhD

A judge with preferences for hard core porn, a police officer investigating a cyber-crime, a politician ordering burn out medication - this kind of very personal and private information is on the market. Get sold to who is willing to pay for.

In a long time experiment, with the help of some social engineering techniques, we were able to get our hands on the most private data you can find on the internet. Click stream data of three million German citizens. They contain every URL they have looked at, every second, every hour, every day for 31 days. In our talk we will not only show how we got that data, but how you can de-anonymize it with some simple techniques.

This data is collected worldwide by big companies, whose legal purpose is to sell analytics and insights for marketers and businesses. In the shadow of Google

PRESENTATIONS

and Facebook, companies have evolved, their names unknown to a broader public but making billions of dollars with your data. The new oil of the 20th century.

Our experiment shows in a drastic way, what the youngest decision reversing the Broadband Privacy Rule means. What the consequences for everyday life could be, when ISPs are allowed to sell your browsing data. And why that piece of regulation from the FCC was so important regarding privacy and constitutional rights.

PANEL - AN EVENING WITH THE EFF

Friday at 20:00 - 22:00 in Trevi Room
Evening Lounge | 0025

Kurt Opsahl, Deputy Executive Director & General Counsel, Electronic Frontier Foundation

Nate Cardozo, EFF Senior Staff Attorney

Eva Galperin, EFF Director of Cyber security

Andrew Crocker, EFF Staff Attorney

Kit Walsh, EFF Staff Attorney

Relax and enjoy in an evening lounge while you get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This Evening Lounge discussion will include updates on current EFF issues such as surveillance online, encryption (and backdoors), and fighting efforts to use intellectual property claims to shut down free speech and halt innovation, discussion of our technology project to protect privacy and speech online, updates on cases and legislation affecting security research, and much more.

ATTACKING AUTONOMIC NETWORKS

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

Omar Eissa, Security Analyst, ERNW GmbH

Autonomic systems are smart systems which do not need any human management or intervention. Cisco is one of the first companies to deploy the technology in which

the routers are just "Plug and Play" with no need for configuration. All that is needed is 5 commands to build fully automated network. It is already supported in pretty much all of the recent software images for enterprise level and carrier grade routers/switches.

This is the bright side of the technology. On the other hand, the configuration is hidden and the interfaces are inaccessible. The protocol is proprietary and there is no mechanism to know what is running within your network.

In this talk, we will have a quick overview on Cisco's Autonomic Network Architecture, then I will reverse-engineer the proprietary protocol through its multiple phases. Finally, multiple vulnerabilities (overall 5) will be presented, one of which allows to crash systems remotely by knowing their IPv6 address.

DEMYSTIFYING WINDOWS KERNEL EXPLOITATION BY ABUSING GDI OBJECTS.

Saturday at 13:00 in 101 Track
45 minutes | Demo, Exploit

SAJF (Saif El-Sherei), Security Analyst, SensePost

Windows kernel exploitation is a difficult field to get into. Learning the field well enough to write your own exploits require full walkthroughs and few of those exist. This talk will do that, release two exploits and a new GDI object abuse technique.

We will provide all the detailed steps taken to develop a full privilege escalation exploit. The process includes reversing a Microsoft's patch, identifying and analyzing two bugs, developing PoCs to trigger them, turning them into code execution and then putting it all together. The result is an exploit for Windows 8.1 x64 using GDI bitmap objects and a new, previously unreleased Windows 7 SP1 x86 exploit involving the abuse of a newly discovered GDI object abuse technique.

CFP REVIEW BOARD

The following collective of awesome individuals helped us review the hundreds of CFP's for DEF CON 25. This year we expanded our boards to include new general reviewers as well as subject matter experts. From February to June these volunteers spent hundreds of hours of their time to pick the best content that fit for DEF CON.

They deserve a big thank you, a cold one to ease the pain, and recognition that you can't please everyone all the time. You can see them at con wearing a CFP review badge.



NIKITA



DT



LEAH



HIGHWIZ



JERICHO



SECBARBIE



ZFASSEL



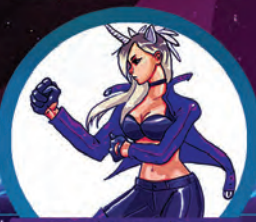
ROAMER



SHAGGY



SUGGY



MALWARE
UNICORN



DEAD ADDICT



WISEACRE



PWCRACK



MEDIC



YAN



SINGE



VULC@N



ZOZ



VYRUS



WEASEL



CRYPT



CLAVIGER



GRIPTER



TOTTENKOPH



BEAKER



CYBERSULU



DAKAHUNA



ASH



MUNIN

SPECIAL REVIEWERS



WISEACRE



PWCRACK



MEDIC



YAN



TUNA



ANDREA



SNOW



MOUSE



WONK

PRESENTATIONS

PANEL- MEET THE FEDS: HOW TO CAUSE SECURITY PROGRESS

Friday at 10:20 in Track 4
75 minutes

Andrea Matwyshyn, Cranky law professor.

Terrell McSweeney, Commissioner, Federal Trade Commission

Dr. Suzanne Schwartz, FDA

Leonard Bailey, Special Counsel for National Security, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice

Lisa Wiswell, Principal at Grimm and a Fellow at the Center for Strategic and International Studies

Making legal and policy progress on security is hard, especially when it involves coordinating with teams inside and across federal agencies/ departments. But, there *are* success stories. DOJ, FDA, FTC, and DoD have all evolved in positive directions in their approach to security over the last five years, engaging more robustly with the security research community. The panelists will introduce their respective agencies/ departments, explain their missions, and describe the evolution of their organizations' approach across time to security and security research. As always, the panelists look forward to answering your questions.



PANEL - MEET THE FEDS (WHO CARE ABOUT SECURITY RESEARCH)

Saturday at 20:00 - 22:00 in Capri Room
Evening Lounge

Allan Friedman, Director of Cybersecurity, National Telecommunications and Information Administration, US Department of Commerce

Amélie E. Koran, Deputy Chief Information Officer for the U.S. Department of Health and Human Services, Office of the Inspector General

Leonard Bailey, Special Counsel for National Security, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice

Nick Leiserson, Legislative Director, Office of Congressman James R. Langevin (RI-02)

Security research is no longer a foreign concept in Washington, DC. A growing number of policymakers are not only thinking about its importance, but are eager to work with hackers to better understand the implications of policy and to help hackers navigate laws that affect security research. Officials from the Department of Commerce, the Department of Justice, and Congress will talk about how security policy has been evolving; help you understand how you can get involved and make your voice heard; and host an extended Q&A. Hear about everything from making laws more hacker friendly to encryption to IoT security. It's your opportunity to meet the feds and ask them anything.

SECURE TOKIN' AND DOOBIEKEYS: HOW TO ROLL YOUR OWN COUNTERFEIT HARDWARE SECURITY DEVICES

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

Joe FitzPatrick, SecuringHardware.com

Michael Leibowitz, Senior Trouble Maker

Let's face it, software security is still in pretty bad shape. We could tell ourselves that everything is fine, but in our hearts, we know the world is on fire. Even as hackers, it's incredibly hard to

know whether your computer, phone, or secure messaging app is pwned. Of course, there's a Solution(tm) - hardware security devices.

We carry authentication tokens not only to secure our banking and corporate VPN connections, but also to access everything from cloud services to social networking. While we've isolated these 'trusted' hardware components from our potentially pwned systems so that they might be more reliable, we will present scenarios against two popular hardware tokens where their trust can be easily undermined. After building our modified and counterfeit devices, we can use them to circumvent intended security assumptions made by their designers and users. In addition to covering technical details about our modifications and counterfeit designs, we'll explore a few attack scenarios for each.

Sharing is Caring, so after showing off a few demonstration, we'll walk you through the process of rolling your own Secure Tokin' and Doobiekey that you can pass around the circle at your next cryptoparty.

SECRET TOOLS: LEARNING ABOUT GOVERNMENT SURVEILLANCE SOFTWARE YOU CAN'T EVER SEE

Friday at 10:00 in Track 4
20 minutes | 0025

Peyton "Foofus" Engel, Attorney at Hurley, Burish & Stanton, S.C.

Imagine that you're accused of a crime, and the basis of the accusation is a log entry generated by a piece of custom software. You might have some questions: does the software work? how accurate is it? how did it get the results that it did? Unfortunately, the software isn't available to the public. And you can't get access to the source code or even a working instance of the software. All you get are assurances that the software is in use by investigators around the globe, and doesn't do anything that law enforcement isn't supposed to be doing. Because you can trust the government, right?

This talk will look at a family of tools designed for investigating peer-to-peer networks. By synthesizing information from dozens of search warrant affidavits, and a few technical sources, we're able to put together at least a partial picture of the software's capabilities. But we'll

PRESENTATIONS

also look at the reasons the government offers for keeping these tools out of the public eye and talk about whether they make sense. Finally, we'll examine the implications that investigations based on secret capabilities have for justice.

BACKDOORING THE LOTTERY AND OTHER SECURITY TALES IN GAMING OVER THE PAST 25 YEARS

Sunday at 11:00 in Track 2
45 minutes

Gus Fritschier, CTO, SeNet International

Evan Teitelman, Engineer, SeNet International

In this talk Gus and Evan will discuss the recent Hot Lotto fraud scandal and how one MUSL employee, Eddie Tipton, was able to rig several state lotteries and win \$17 million (or perhaps more). Gus' firm is actively supporting the prosecution in this case. Evan was responsible for identifying and analyzing how Eddie was able to rig the RNG.

Details on the rigged RNG and other details from the case will be presented publicly for the first time during this talk.

For historical context other related attacks including the Ron Harris and hacking keno in the 1990's and a recent incident involving a Russian hacking syndicate's exploitation of slot machines will also be discussed.

MEATPISTOL, A MODULAR MALWARE IMPLANT FRAMEWORK

Friday at 17:00 in Track 3
45 minutes | Demo, Tool

FuzzyNop (Josh Schwartz), Director of Offensive Security @ Salesforce
ceyx (John Cramb), Hacker

Attention Red Teamers, Penetration Testers, and Offensive Security Operators, isn't the overhead of fighting attribution, spinning up infrastructure, and having to constantly re-write malware an absolute pain and timesink!?! It was for us too, so we're fixing that for good (well, maybe for evil). Join us for the public unveiling and open source release of our latest project, MEATPISTOL, a modular malware framework for

implant creation, infrastructure automation, and shell interaction. This framework is designed to meet the needs of offensive security operators requiring rapid configuration and creation of long lived malware implants and associated command and control infrastructure. Say goodbye to writing janky one-off malware and say hello to building upon a framework designed to support efficient yolo-scoped adversarial campaigns against capable targets.

CALL THE PLUMBER - YOU HAVE A LEAK IN YOUR NAMED PIPE

Sunday at 14:00 in 101 Track
45 minutes | Demo

Gil Cohen, CTO, Comsec group

The typical security professional is largely unfamiliar with the Windows named pipes interface, or considers it to be an internal-only communication interface. As a result, open RPC (135) or SMB (445) ports are typically considered potentially entry points in "infrastructure" penetration tests.

However, named pipes can in fact be used as an application-level entry vector for well known attacks such as buffer overflow, denial of service or even code injection attacks and XML bombs, depending on the nature of listening service to the specific pipe on the target machine.

As it turns out, it seems that many popular and widely used Microsoft Windows-based enterprise applications open a large number of named pipes on each endpoint or server on which they are deployed, significantly increase an environment's attack surface without the organization or end user being aware of the risk. Since there's a complete lack of awareness to the entry point, there's very limited options available to organizations to mitigate it, making it a perfect attack target for the sophisticated attacker.

In this presentation we will highlight how named pipes have become a neglected and forgotten external interface. We will show some tools that can help find vulnerable named pipes, discuss the mitigations, and demonstrate the exploitation process on a vulnerable interface.

I KNOW WHAT YOU ARE BY THE SMELL OF YOUR WIFI

Sunday at 10:00 in Track 2
20 minutes | Art of Defense, Demo, Tool, Audience Participation

Denton Gentry, Software Engineer

Existing fingerprinting mechanisms to identify client devices on a network tend to be coarse in their identification. For example they can tell it is an iPhone of some kind, or that it is a Samsung Android device of some model. They might look at DHCP information to know its OS, see if the client responds to SSDP, or check DNS-SD TXT responses.

By examining Wi-Fi Management frames we can identify the device much more specifically. We can tell a iPhone 5S from an iPhone 5, a Samsung Galaxy S8 from an S7, an LG G5 from a G4. This talk describes how the signature mechanism works.

Specifically identifying the client is the first step toward further scanning or analysis of that client's behavior on the network.

INTRODUCING HUNT: DATA DRIVEN WEB HACKING & MANUAL TESTING

Saturday at 17:00 in Track 3
45 minutes | Demo, Tool

Jason Haddix, Head of Trust and Security @ Bugcrowd

What if you could super-charge your web hacking? Not through pure automation (since it can miss so much) but through powerful alerts created from real threat intelligence? What if you had a Burp plugin that did this for you? What if that plugin not only told you where to look for vulns but also gave you curated resources for additional exploitation and methodology? What if you could organize your web hacking methodology inside of your tools? Well, now you do! HUNT is a new Burp Suite extension that aims to arm web hackers with parameter level suggestions on where to look for certain classes of vulnerabilities (SQLi, CMDi, LFI/RFI, and more!). This data is parsed from hundreds of real-world assessments, providing the user with the means to effectively root out critical issues. Not only will HUNT help you assess large targets more thoroughly but it also aims to organize common web hacking

PRESENTATIONS

methodologies right inside of Burp suite. As an open source project, we will go over the data driven design of HUNT and it's core functionality.

OPT OUT OR DEATH TRYING I- ANTI-TRACKING BOTS RADIOS AND KEYSTROKE INJECTION

Thursday at 11:00 in 101 Track 2
45 minutes | 0025, Demo, Tool, Exploit

Weston Hecker, Principal Application Security Engineer, "NCR"

It's hard not to use a service now days that doesn't track your every move and keystroke if you absolutely must use these systems why not give them the most useless information possible. Along with the fact that several companies are tracking their customers online now they are taking it to physical brick and mortar stores this talk will be geared looking at the attack surface of instore tracking and attacking these systems for the purpose of overloading their systems or making the information so inaccurate that it becomes useless. Watch as a 32 year old hackers online profile is turned to that of a 12 year old girl who loves horses!

TRACKING SPIES IN THE SKIES

Saturday at 15:00 in Track 2
45 minutes | Art of Defense, 0025, Tool

Jason Hernandez, Hacker / Technical Editor, North Star Post

Sam Richards, Editor and Journalist, North Star Post

Jerod MacDonald-Evoy, Journalist, North Star Post

Law enforcement agencies have used aircraft for decades to conduct surveillance, but modern radio, camera, and electronics technology has dramatically expanded the power and scope of police surveillance capabilities. The Iraq War and other conflicts have spurred the development of mass surveillance technologies and techniques that are now widely available to domestic police. The FBI, DEA, and other agencies flew powerful surveillance aircraft over cities for years in relative secrecy before breaking in to public attention in 2015. This presentation will discuss the capabilities of these aircraft, the

discovery of the FBI and others' surveillance fleets, and continued efforts to shed light on aerial surveillance. We will discuss a method for detecting surveillance indicators in real time based on mutilation of aggregated ADS-B data, and introduce code for detecting surveillance indicators from flight behavior.

GET \$FWND: ATTACKING BATTLE-HARDENED WINDOWS SERVER

Saturday at 10:00 in Track 3
20 minutes | Demo, Tool

Lee Holmes, Principal Security Architect, Microsoft

Windows Server has introduced major advances in remote management hardening in recent years through PowerShell Just Enough Administration ("JEA"). When set up correctly, hardened JEA endpoints can provide a formidable barrier for attackers: whitelisted commands, with no administrative access to the underlying operating system.

In this presentation, watch as we show how to systematically destroy these hardened endpoints by exploiting insecure coding practices and administrative complexity.

BYPASSING ANDROID PASSWORD MANAGER APPS WITHOUT ROOT

Sunday at 13:00 in Track 2
45 minutes | Demo, Exploit

Stephan Huber, Fraunhofer SIT

Siegfried Rasthofer, Fraunhofer SIT

Security experts recommend using different, complex passwords for individual services, but everybody knows the issue arising from this approach: It is impossible to keep all the complex passwords in mind. One solution to this issue are password managers, which aim to provide a secure, centralized storage for credentials. The rise of mobile password managers even allows the user to carry their credentials in their pocket, providing instant access to these credentials if required. This advantage can immediately turn into a disadvantage as all credentials are stored in one central location.

What happens if your device gets lost, stolen or a hacker gets access to your device? Are your personal secrets and credentials secure?

We say no! In our recent analysis of well-known Android password manager apps, amongst them are vendors such as LastPass, Dashlane, 1Password, Avast, and several others, we aimed to bypass their security by either stealing the master password or by directly accessing the stored credentials. Implementation flaws resulted in severe security vulnerabilities. In all of those cases, no root permissions were required for a successful attack. We will explain our attacks in detail. We will also propose possible security fixes and recommendations on how to avoid the vulnerabilities.

AMATEUR DIGITAL ARCHEOLOGY

Thursday at 13:00 in 101 Track
45 minutes

Matt 'openfly' Joyce, Hacker at NYC Resistor

'Digital Archeology' is actually the name of a Digital Forensics text book. But what if we used forensics techniques targeting cyber crime investigations to help address the void in Archeology that addresses digital media and silicon artifacts. At NYC Resistor in Brooklyn we've gotten into the world of Digital Archeology on several occasions and the projects have been enjoyable and educational.

Now, imagine what could happen if a bunch of hackers are able to get their hands on a laptop pulled off of a space shuttle.

Then come to our talk and find out what ACTUALLY happened. I bought a laptop at auction that claimed to be off a Shuttle Mission. It turns out to have been mostly authentic. This will be a little foray into the history of this device and what I could find out about it, and how I did that.

Spoiler Alert: We found out a lot.

Bonus: I may have found the sister laptop of this laptop (serial numbers match)

CUNDFUCKING FORENSICS: ACTIVE/PASSIVE (I.E. OFFENSIVE/DEFENSIVE) MEMORY HACKING/DEBUGGING.

Saturday at 10:20 in Track 4
20 minutes | Hacker History, Art of Defense, Demo, Tool

K2, Director, IOACTIVE

How to forensic, how to fuck forensics and how to un-fuck cyber forensics.

Defense: WTF is a RoP, why I care and how to detect it statically from memory. Counteract "Gargoyle" attacks.

Defense: For one of DEF CON 24's more popular anti-forensics talks (see int0x80 - Anti Forensics). In memory (passive debugging) techniques that allows for covert debugging of attackers (active passive means that we will (try hard to) not use events or methods that facilities are detectable by attackers).

Offense: CloudLeech - a cloud twist to Ulf Frisk Direct Memory Attack

HACKING DEMOCRACY

Friday at 20:00 - 22:00 in Capri Room
Evening Lounge

Mr. Sean Kanuck, Stanford University, Center for International Security and Cooperation

Are you curious about the impact of fake news and influence operations on elections? Are you concerned about the vulnerability of democratic institutions, the media, and civil society? Then come engage with your peers and the first US National Intelligence Officer for Cyber Issues on ways to hack democracy. He will: (1) provide a low-tech, strategic analysis of recent events, foreign intelligence threats, and the future of information warfare; (2) lead a Socratic dialogue with attendees about the trade-offs between national security and core democratic values (such as freedom, equality, and privacy); and (3) open the floor to audience questions and/or a moderated group debate.

This session is intended to be informal and participatory. It will cover a range of issues from supply chain attacks on voting machines to psychological operations by using an

interdisciplinary approach that encompasses constitutional law, world history, game theory, social engineering, and international affairs. The discussion will occur against the backdrop of cyber security and critical infrastructure protection, but it will not examine any specific hardware or software systems; rather, it will concern the conceptual formulation and conduct of modern strategic influence campaigns. No specific knowledge is required, but a skeptical mind and mischievous intellect are a must.

HACKING DEMOCRACY: A SOCRATIC DIALOGUE

Friday at 12:00 in Track 4
45 minutes

Mr. Sean Kanuck, Stanford University, Center for International Security and Cooperation

In the wake of recent presidential elections in the US and France, "hacking" has taken on new political and social dimensions around the globe. We are now faced with a world of complex influence operations and dubious integrity of information. What does that imply for democratic institutions, legitimacy, and public confidence?

This session will explore how liberal democracy can be hacked — ranging from direct manipulation of electronic voting tallies or voter registration lists to indirect influence over mass media and voter preferences — and question the future role of "truth" in open societies. Both domestic partisan activities and foreign interventions will be considered on technical, legal, and philosophical grounds. The speaker will build on his experience as an intelligence professional to analyze foreign capabilities and intentions in the cyber sphere in order to forecast the future of information warfare. Audience members will be engaged in a Socratic dialogue to think through how modern technologies can be used to propagate memes and influence the electorate. The feasibility of, and public policy challenges associated with, various approaches to hacking democracy will also be considered. This conceptual discussion of strategic influence campaigns will not require any specific technical or legal knowledge.

HACKING SMART CONTRACTS

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

Konstantinos Karagiannis, Chief Technology Officer, Security Consulting, BT Americas

It can be argued that the DAO hack of June 2016 was the moment smart contracts entered mainstream awareness in the InfoSec community. Was the hope of taking blockchain from mere cryptocurrency platform to one that can perform amazing Turing-complete functions doomed? We've learned quite a lot from that attack against contract code, and Ethereum marches on. Smart contracts are a key part of the applications being created by the Enterprise Ethereum Alliance, Quorum, and smaller projects in financial and other companies. Ethical hacking of smart contracts is a critical new service that is needed. And as is the case with coders of Solidity (the language of Ethereum smart contracts), hackers able to find security flaws in the code are in high demand.

Join Konstantinos for an introduction to a methodology that can be applied to Solidity code review ... and potentially adapted to other smart contract projects. We'll examine the few tools that are needed, as well as the six most common types of flaws, illustrated using either public or sanitized real world" vulnerabilities.

THE BRAIN'S LAST STAND

Friday at 10:00 in Track 3
45 minutes

Garry Kasparov, Avast Security Ambassador

Former world chess champion Garry Kasparov has a unique place in history as the proverbial "man" in "man vs. machine" thanks to his iconic matches against the IBM supercomputer Deep Blue. Kasparov walked away from that watershed moment in artificial intelligence history with a passion for finding ways humans and intelligent machines could work together. In the spirit of "if you can't beat 'em, join 'em," Kasparov has explored that potential for the 20 years since his loss to Deep Blue. Navigating a practical and hopeful approach between the utopian and dystopian camps, Kasparov focuses on how we can rise to the challenge of the AI revolution despite job losses to automation.

PRESENTATIONS

and refuting those who say our technology is making us less human. He includes concrete examples and forward-looking strategies on AI.

HORROR STORIES OF A TRANSLATOR AND HOW A TWEET CAN START A WAR WITH LESS THAN 140 CHARACTERS

Friday at 20:00 - 22:00 in Modena Evening Lounge

El Kentaro, Hacker

Translators are invisible, when they are present it is assumed that they know the language and are accurately translating between the languages. But how do you assure that the translator is accurately translating or working without an agenda? Although many of the case studies presented in this talk will focus on translating between different languages, the basic premise can be applied in any case where information needs to be shared among 2 or more different contexts. (i.e.: Sales vs Engineering, Government vs Private sector etc) . The talk will showcase publicly known historical cases and personal experiences where translation errors (accidental and deliberate) have lead to misunderstandings some with dire consequences. Also the talk will showcase using translators as an offensive tool (i.e.:How to create more credible fake news). We as a society consume more information and consume it faster than before, we have to be aware of the dangers that are inherit with bad translations. Also the infosec/cyber security profession because of the potential for large scale global impacts and or the need to maintain operational security poses unique considerations when translating or using a translator. This talk will highlight the unique challenges of using a translator or translations in such environments.

RADIO EXPLOITATION 101: CHARACTERIZING, CONTEXTUALIZING, AND APPLYING WIRELESS ATTACK METHODS

Friday at 16:00 in 101 Track
45 minutes | Demo

Matt Knight, Senior Software Engineer, Threat Research at Bastille

Marc Newlin, Security Researcher at Bastille

What do the Dallas tornado siren attack, hacked electric skateboards, and insecure smart door locks have in common? Vulnerable wireless protocols. Exploitation of wireless devices is growing increasingly common, thanks to the proliferation of radio frequency protocols driven by mobile and IoT. While non-Wi-Fi and non-Bluetooth RF protocols remain a mystery to many security practitioners, exploiting them is easier than one might think.

Join us as we walk through the fundamentals of radio exploitation. After introducing essential RF concepts and characteristics, we will develop a wireless threat taxonomy by analyzing and classifying different methods of attack. As we introduce each new attack, we will draw parallels to similar wired network exploits, and highlight attack primitives that are unique to RF. To illustrate these concepts, we will show each attack in practice with a series of live demos built on software-defined and hardware radios.

Attendees will come away from this session with an understanding of the mechanics of wireless network exploitation, and an awareness of how they can bridge their IP network exploitation skills to the wireless domain.

PERSISTING WITH MICROSOFT OFFICE: ABUSING EXTENSIBILITY OPTIONS

Saturday at 10:00 in 101 Track
20 minutes | Demo

William Knowles, MWR InfoSecurity

One software product that red teamers will almost certainly find on any compromised workstation is Microsoft Office. This talk will discuss the ways that native functionality

within Office can be abused to obtain persistence. The following opportunities for Office-based persistence will be discussed:

- (1) WLL and XLL add-ins for Word and Excel - a legacy add-in that allows arbitrary DLL loading.
- (2) VBA add-ins for Excel and PowerPoint - an alternative to backdoored template files, which executes whenever the applications load.
- (3) COM add-ins for all Office products - an older cross-application add-in that leverages COM objects.
- (4) Automation add-ins for Excel - user defined functions that allow command execution through spreadsheet formulae.
- (5) VBA editor (VBE) add-ins for all VBA using Office products - executing commands when someone tries to catch you using VBA to execute commands.
- (6) VSTO add-ins for all Office products - the newer cross-application add-in that leverages a special Visual Studio runtime.

Each persistence mechanism will be discussed in terms of its relative advantages and disadvantages for red teamers. In particular, with regards to their complexity to deploy, privilege requirements, and applicability to Virtual Desktop Infrastructure (VDI) environments which hinder the use of many traditional persistence mechanisms.

The talk isn't all red - there's also some blue to satisfy the threat hunters and incident responders amongst us. The talk will finish with approaches to detection and prevention of these persistence mechanisms.

CISCO CATALYST EXPLOITATION

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

Artem Kondratenko, Penetration Tester, Security Researcher

On March 17th, Cisco Systems Inc. made a public announcement that over 300 of the switches it manufactures are prone to a critical vulnerability that allows a potential attacker to take full control of the network equipment.

This damaging public announcement was preceded by Wikileaks' publication of documents codenamed as "Vault 7" which contained information on vulnerabilities and description of tools needed to access phones, network equipment and even IOT devices.

Cisco Systems Inc. had a huge task in front of them - patching this vast amount of different switch models is not an easy task. The remediation for this vulnerability was available with the initial advisory and patched versions of IOS software were announced on May 8th 2017.

We all heard about modern exploit mitigation techniques such as Data Execution Prevention, Layout Randomization. But just how hardened is the network equipment? And how hard is it to find critical vulnerabilities?

To answer that question I decided to reproduce the steps necessary to create a fully working tool to get remote code execution on Cisco switches mentioned in the public announcement.

This presentation is a detailed write-up of the exploit development process for the vulnerability in Cisco Cluster Management Protocol that allows a full takeover of the device.

THE ADVENTURES OF AV AND THE LEAKY SANDBOX

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

Itzik Kotler, Co-Founder & CTO, SafeBreach

Amit Klein, VP Security Research, SafeBreach

Everyone loves cloud-AV. Why not harness the wisdom of clouds to protect the enterprise? Consider a high-security enterprise with strict egress filtering - endpoints have no direct Internet connection, or the endpoints' connection to the Internet is restricted to hosts used by their legitimately installed software. Let's say there's malware running on an endpoint with full privileges. The malware still can't exfiltrate data due to the strict egress filtering.

Now let's also assume that this enterprise uses cloud-enhanced anti-virus (AV). You'd argue that if malware is already running on the endpoint with full privileges, then an AV agent can't degrade the security of the endpoint. And you'd be completely wrong.

In this presentation, we describe and demonstrate a novel technique for exfiltrating data from highly secure enterprises which employ strict egress filtering. Assuming the endpoint has a cloud-enhanced antivirus installed, we show that if the AV employs an Internet-connected sandbox in its cloud, it in fact facilitates such exfiltration. We release a tool implementing the exfiltration technique, and provide real-world results from several prominent AV products. We also provide insights on AV in-the-cloud sandboxes. Finally we address the issues of how to further enhance the attack, and possible mitigations.

THE SPEAR TO BREAK THE SECURITY WALL OF S7COMMPLUS

Saturday at 10:00 in Track 4
20 minutes | Exploit

Cheng, ICS Security Researcher, NSF0CUS

In the past few years, attacks against industrial control systems (ICS) have increased year over year. Stuxnet in 2010 exploited the insecurity of the S7Comm protocol, the communication protocol used between Siemens Simatic S7 PLCs to cause serious damage in nuclear power facilities. After the exposure of Stuxnet, Siemens has implemented some security reinforcements into the S7Comm protocol. The current S7CommPlus protocol implementing encryption has been used in S7-1200 V4.0 and above, as well as S7-1500, to prevent attackers from controlling and damaging the PLC devices. Is the current S7CommPlus a real high security protocol? This talk will demonstrate a spear that can break the security wall of the S7CommPlus protocol. First, we use software like Wireshark to analyze the communications between the Siemens TIA Portal and PLC devices. Then, using reverse debugging software like WinDbg and IDA we can break the encryption in the S7CommPlus protocol. Finally, we write a MFC program which can control the start and the stop of the PLC, as well as value changes of PLC's digital and analog inputs & outputs. Based on the research above, we present two security proposals at both code level and protocol level to improve the security of Siemens PLC devices.

UNCOVERING USEFUL AND EMBARRASSING INFO WITH MALTEGO

Standby Speakers at in
45 minutes | Demo

Andrew MacPherson, Ops/Dev - Paterva

The talk has two sections - useful and embarrassing.

In the 'useful' section of this fun filled talk we show how we combine the power of Maltego and Shodan to hunt for ICS devices on the Internet. We tackle the difficult problem of finding the function, owners and locations of these devices using OSINT and Maltego. The result is a one click sequence of transforms that makes finding interesting ICS devices child's play. In the 'embarrassing' section we look at how network footprinting (which we've refined to an art in Maltego) becomes useful for identifying and profiling people who's job description involves lots of lies and who probably does not want to be associated with the data that's out there on them.

CONTROLLING IOT DEVICES WITH CRAFTED RADIO SIGNALS

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

Caleb Madrigal, Hacker, FireEye/Mandiant

In this talk, we'll be exploring how wireless communication works. We'll capture digital data live (with Software-Defined Radio), and see how the actual bits are transmitted. From here, we'll see how to view, listen to, manipulate, and replay wireless signals. We'll also look at interrupting wireless communication, and finally, we'll even generate new radio waves from scratch (which can be useful for fuzzing and brute force attacks). I'll also be demoing some brand new tools I've written to help in the interception, manipulation, and generation of digital wireless signals with SDR.



PRESENTATIONS

REAL-TIME RFID CLONING IN THE FIELD

Thursday at 15:00 in 101 Track 2
20 minutes | Demo, Tool, Audience Participation

Dennis Maldonado, Adversarial Engineer - LARES Consulting

Ever been on a job that required you to clone live RFID credentials? There are many different solutions to cloning RFID in the field and they all work fine, but the process can be slow, tedious, and error prone. What if there was a new way of cloning badges that solved these problems? In this presentation, we will discuss a smarter way for cloning RFID in the field that is vastly more efficient, useful, and just plain cool. We will go over the current tools and methods for long-range RFID cloning, then discuss and demonstrate a new method that will allow you to clone RFID credentials in the field in just seconds, changing the way you perform red team engagements forever.

TWENTY YEARS OF MMORPG HACKING: BETTER GRAPHICS, SAME EXPLOITS

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

Manfred (@_EBFE), Security Analyst at Independent Security Evaluators

In theme with this year's DEF CON this presentation goes through a 20 year history of exploiting massively multiplayer online role-playing games (MMORPGs). The presentation technically analyzes some of the virtual economy-devastating, low-hanging-fruit exploits that are common in nearly every MMORPG released to date. The presenter, Manfred (@_EBFE), goes over his adventures in hacking online games starting with 1997's Ultima Online and subsequent games such as Dark Age of Camelot, Anarchy Online, Asherons Call 2, ShadowBane, Lineage II, Final Fantasy XI/XIV, World of Warcraft, plus some more recent titles such as Guild Wars 2 and Elder Scrolls Online and many more!

The presentation briefly covers the exploit development versus exploit detection/prevention arms race and its current state. Detailed

packet analysis and inference on what the code looks like server side in order for some of the exploits to be possible is presented.

This presentation includes a live demonstration of at least one unreleased exploit to create mass amounts of virtual currency in a recent and popular MMORPG.

MALICIOUS CDNS: IDENTIFYING ZBOT DOMAINS EN MASSE VIA SSL CERTIFICATES AND BIPARTITE GRAPHS

Sunday at 13:00 in Track 3
45 minutes | Art of Defense

Thomas Mathew, OpenDNS (Cisco)

Dhia Mahjoub, Head of Security Research, Cisco Umbrella (OpenDNS)

Prior research detailing the relationship between malware, bulletproof hosting, and SSL gave researchers methods to investigate SSL data only if given a set of seed domains. We present a novel statistical technique that allow us to discover botnet and bulletproof hosting IP space by examining SSL distribution patterns from open source data while working with limited or no seed information. This work can be accomplished using open source datasets and data tools.

SSL data obtained from scanning the entire IPv4 namespace can be represented as a series of 4 million node bipartite graphs where a common name is connected to either an IP/CIDR/ASN via an edge. We use the concept of relative entropy to create a pairwise distance metric between any two common names and any two ASNs. The metric allows us to generalize the concept of regular and anomalous SSL distribution patterns.

Relative entropy is useful in identifying domains that have anomalous network structures. The domains we found in this case were related to the Zbot proxy network. The Zbot proxy network contains a structure similar to popular CDNs like Akamai, Google, etc but instead rely on compromised devices to relay their data. Through layering these SSL signals with passive DNS data we create a pipeline that can extract Zbot domains with high accuracy.

TROJAN-TOLERANT HARDWARE & SUPPLY CHAIN SECURITY IN PRACTICE

Saturday at 14:00 in Track 2
45 minutes | Art of Defense, Demo, Tool

Vasilios Mavroudis, Doctoral Researcher, University College London

Dan Cvrcek, Co-founder, Enigma Bridge Ltd

The current consensus within the security industry is that high-assurance systems cannot tolerate the presence of compromised hardware components. In this talk, we challenge this perception and demonstrate how trusted, high-assurance hardware can be built from untrusted and potentially malicious components.

The majority of IC vendors outsource the fabrication of their designs to facilities overseas, and rely on post-fabrication tests to weed out deficient chips. However, such tests are not effective against: 1) subtle unintentional errors (e.g., malfunctioning RNGs) and 2) malicious circuitry (e.g., stealthy Hardware Trojans). Such errors are very hard to detect and require constant upgrades of expensive forensics equipment, which contradicts the motives of fabrication outsourcing.

In this session, we introduce a high-level architecture that can tolerate multiple, malicious hardware components, and outline a new approach in hardware compromises risk management. We first demo our backdoor-tolerant Hardware Security Module built from low-cost commercial off-the-shelf components, benchmark its performance, and delve into its internals. We then explain the importance of "component diversification" and "non-overlapping supply chains", and finally discuss how "mutual distrust" can be exploited to further reduce the capabilities of the adversaries.

WHERE ARE THE SDN SECURITY TALKS?

Thursday at 10:00 in 101 Track 2
45 minutes | Demo, Tool

Jon Medina, Protiviti

Software Defined Networking is no longer a fledgling technology. Google, Amazon, Facebook, and Verizon all rely on the scalability, programmability, flexibility, availability, and yes, security provided by SDN. So why has there only ever been one DEF CON speaker presenting on SDN and security?

This talk will provide a brief introduction to SDN and security, demonstrate ways of compromising and securing a Software Defined Network and will illustrate new ways of using the power of open source SDN coupled with machine learning to maintain self-defending networks.

EXPLOITING OLD MAG-STRIPE INFORMATION WITH NEW TECHNOLOGY

Thursday at 15:20 in 101 Track 2
20 minutes | Demo, Tool, Exploit

Salvador Mendoza, Hacker

A massive attack against old magnetic stripe information could be executed with precision implementing new technology. In the past, a malicious individual could spoof magstripe data but in a slow and difficult way. Also brute force attacks were tedious and time-consuming. Technology like Bluetooth could be used today to make a persistent attack in multiple magnetic card readers at the same time with audio spoof.

Private companies, banks, trains, subways, hotels, schools and many others services are still using magstripe information to even make monetary transactions, authorize access or to generate "new" protocols like MST(Magnetic Secure Transmission) During decades the exploitation of magstripe information was an acceptable risk for many companies because the difficulty to achieve massive attacks simultaneously was not factible. But today is different.

Transmitting magstripe information in audio files is the faster and easier way to make a cross-platform magstripe spoofer. But how an attacker could transmit the audio spoof information to many magnetic card readers at the same time?

PRESENTATIONS

In this talk, we will discuss how an attacker could send specific data or achieve a magstripe jammer for credit card terminals, PoS or any card reader. Also, how it could be implemented to generate brute force attacks against hotel door locks or tokenization processes as examples.

'TICK, TICK, TICK. BOOM! YOU'RE DEAD.' -- TECH & THE FTC

Friday at 16:00 in Track 4
45 minutes

Whitney Merrill, Privacy, eCommerce & Consumer Protection Counsel, Electronic Arts

Terrell McSweeney, Commissioner, Federal Trade Commission

The Federal Trade Commission is a law enforcement agency tasked with protecting consumers from unfair and deceptive practices. Protecting consumers on the Internet and from bad tech is nothing new for the FTC. We will take a look back at what the FTC was doing when DEF CON first began in 1993, and what we've been doing since. We will discuss enforcement actions involving modem hijacking, FUD advertising, identity theft, and even introduce you to Dewie the e-Turtle. Looking forward, we will talk about the FTC's future protecting consumers' privacy and data security and what you can do to help.

FRIDAY THE 13TH: JSON ATTACKS!

Sunday at 14:00 in Track 4
45 minutes | Demo, Exploit

Alvaro Muñoz, Principal Security Researcher, Hewlett Packard Enterprise

Oleksandr Mirosh, Senior Security QA Engineer, Hewlett Packard Enterprise

2016 was the year of Java deserialization apocalypse. Although Java Deserialization attacks were known for years, the publication of the Apache Commons Collection Remote Code Execution (RCE from now on) gadget finally brought this forgotten vulnerability to the spotlight and motivated the community to start finding and fixing these issues.

One of the most suggested solutions for avoiding Java deserialization issues was to move away from Java Deserialization altogether and use

safer formats such as JSON. In this talk, we will analyze the most popular JSON parsers in both .NET and Java for potential RCE vectors.

We will demonstrate that RCE is also possible in these libraries and present details about the ones that are vulnerable to RCE by default. We will also discuss common configurations that make other libraries vulnerable.

In addition to focusing on JSON format, we will generalize the attack techniques to other serialization formats. In particular, we will pay close attention to several serialization formats in .NET. These formats have also been known to be vulnerable since 2012 but the lack of known RCE gadgets led some software vendors to not take this issue seriously. We hope this talk will change this. With the intention of bringing the due attention to this vulnerability class in .NET, we will review the known vulnerable formats, present other formats which we found to be vulnerable as well and conclude presenting several gadgets from system libraries that may be used to achieve RCE in a stable way: no memory corruption – just simple process invocation.

Finally, we will provide recommendations on how to determine if your code is vulnerable, provide remediation advice, and discuss alternative approaches.

CABLETAP: WIRELESSLY TAPPING YOUR HOME NETWORK

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

Marc Newlin, Security Researcher at Bastille Networks

Logan Lamb, Security Researcher at Bastille Networks

Chris Grayson, Founder and Principal Engineer at Web Sight.IO

Abstract will be released prior to DEF CON.

PRESENTATIONS

DNS - DEVIANT NAME SERVICES - DESTROYING PRIVACY & ANONYMITY WITHOUT YOUR CONSENT

Saturday at 12:00 in Track 3
45 minutes | Art of Defense

Jim Nitterauer, Senior Security Specialist, AppRiver, LLC

You've planned this engagement for weeks. Everything's mapped out. You have tested all your proxy and VPN connections. You are confident your anonymity will be protected. You fire off the first round and begin attacking your target. Suddenly something goes south. Your access to the target site is completely blocked no matter what proxy or VPN you use. Soon, your ISP contacts you reminding you of their TOS while referencing complaints from the target of your engagement. You quickly switch MAC addresses and retry only to find that you are quickly blocked again!

What happened? How were you betrayed? The culprit? Your dastardly DNS resolvers and more specifically, the use of certain EDNSO options by those resolvers.

This presentation will cover the ways in which EDNS OPT code data can divulge details about your online activity, look at methods for discovering implementation by upstream DNS providers and discuss ways in which malicious actors can abuse these features. We will also examine steps you can take to protect yourself from these invasive disclosures.

The details covered will be only moderately technical. Having a basic understanding of RFC 6891 and general DNS processes will help in understanding. We will discuss the use of basic tools including Wireshark, Packetbeat, Graylog and Dig.

LINUX-STACK BASED V2X FRAMEWORK: ALL YOU NEED TO HACK CONNECTED VEHICLES

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

p3n3troot0r (Duncan Woodbury), Hacker

ginsback (Nicholas Haltmeyer), Hacker

Vehicle-to-vehicle (V2V) and, more generally, vehicle-to-everything (V2X) wireless communications enable semi-autonomous driving via the exchange of state information between a network of connected vehicles and infrastructure units. Following 10+ years of standards development, particularly of IEEE 802.11p and the IEEE 1609 family, a lack of available implementations has prevented the involvement of the security community in development and testing of these standards. Analysis of the WAVE/DSRC protocols in their existing form reveals the presence of vulnerabilities which have the potential to render the protocol unfit for use in safety-critical systems. We present a complete Linux-stack based implementation of IEEE 802.11p and IEEE 1609.3/4 which provide a means for hackers and academics to participate in the engineering of secure standards for intelligent transportation systems.

WEAPONIZING MACHINE LEARNING: HUMANITY WAS OVERRATED ANYWAY

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

Dan "AltF4" Petro, Senior Security Associate, Bishop Fox

Ben Morris, Security Analyst, Bishop Fox

At risk of appearing like mad scientists, reveling in our latest unholy creation, we proudly introduce you to DeepHack: the open-source hacking AI. This bot learns how to break into web applications using a neural network, trial-and-error, and a frightening disregard for humankind.

DeepHack can ruin your day without any prior knowledge of apps, databases - or really anything else. Using just one algorithm, it learns

how to exploit multiple kinds of vulnerabilities, opening the door for a host of hacking artificial intelligence systems in the future.

This is only the beginning of the end, though. AI-based hacking tools are emerging as a class of technology that pentesters have yet to fully explore. We guarantee that you'll be either writing machine learning hacking tools next year, or desperately attempting to defend against them.

No longer relegated just to the domain of evil geniuses, the inevitable AI dystopia is accessible to you today! So join us and we'll demonstrate how you too can help usher in the destruction of humanity by building weaponized machine learning systems of your own - unless time travelers from the future don't stop us first.

TEACHING OLD SHELLCODE NEW TRICKS

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

Josh Pitts, Hacker

Metasploit x86 shellcode has been defeated by EMET and other techniques not only in exploit payloads but through using those payloads in non-exploit situations (e.g. binary payload generation, PowerShell deployment, etc.). This talk describes taking Metasploit payloads (minus Stephen Fewer's hash API), incorporating techniques to bypass Caller/EAF[*] checks (post ASLR/DEP bypass) and merging those techniques together with automation to make something better.

POPPING A SMART GUN

Saturday at 17:00 in Track 4
45 minutes | Demo, Exploit

Plorer, Hacker

Smart guns are sold with a promise: they can be fired only by authorized parties. That works in the movies, but what about in real life? In this talk, we explore the security of one of the only smart guns available for sale in the world. Three vulnerabilities will be demonstrated. First, we will show how to make the weapon fire even when separated from its owner by a considerable distance. Second, we will show how to prevent the weapon from firing even when authorized by its owner. Third, we will show how to fire the

weapon even when not authorized by its owner, with no prior contact with the specific weapon, and with no modifications to the weapon.

DIGITAL VENGEANCE: EXPLOITING THE MOST NOTORIOUS C&C TOOLKITS

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

Professor Plum, Hacker

Every year thousands of organizations are compromised by targeted attacks. In many cases the attacks are labeled as advanced and persistent which suggests a high level of sophistication in the attack and tools used. Many times, this title is leveraged as an excuse that the events were inevitable or irresistible, as if the assailants' skill set is well beyond what defenders are capable of. To the contrary, often these assailants are not as untouchable as many would believe.

If one looks at the many APT reports that have been released over the years some clear patterns start to emerge. A small number of Remote Administration Tools are preferred by actors and reused across multiple campaigns. Frequently sited tools include Gh0st RAT, Plug-X, and XtremeRAT among others. Upon examination, the command and control components of these notorious RATs are riddled with vulnerabilities. Vulnerabilities that can be exploited to turn the tables from hunter to hunted.

The presentation will disclose several exploits that could allow remote execution or remote information disclosure on computers running these well-known C&C components. It should serve as a warning to those actors who utilize such toolsets. That is to say, such actors live in glass houses and should stop throwing stones.

PRESENTATIONS

THE INTERNET ALREADY KNOWS I'M PREGNANT

Friday at 17:00 in Track 4
45 minutes | Exploit

Cooper Quintin, Staff Technologist - EFF

Kashmir Hill, Journalist - Gizmodo Media

Women's health is big business. There are a staggering number of applications for Android to help people keep track of their monthly cycle, know when they may be fertile, or track the status of their pregnancy. These apps entice the user to input the most intimate details of their lives, such as their mood, sexual activity, physical activity, physical symptoms, height, weight, and more. But how private are these apps, and how secure are they really? After all, if an app has such intimate details about our private lives it would make sense to ensure that it is not sharing those details with anyone such as another company or an abusive partner/parent. To this end EFF and Journalist Kashmir Hill have taken a look at some of the privacy and security properties of over a dozen different fertility and pregnancy tracking apps. Through our research we have uncovered several privacy issues in many of the applications as well as some notable security flaws as well as a couple of interesting security features.

FROM "ONE COUNTRY - ONE FLOPPY" TO "STARTUP NATION" - THE STORY OF THE EARLY DAYS OF THE ISRAELI HACKING COMMUNITY, AND THE JOURNEY TOWARDS TODAY'S VIBRANT STARTUP SCENE

Saturday at 16:00 in Track 2
45 minutes | Hacker History

Inbar Raz, Principal Researcher, PerimeterX Inc.

Eden Shochat, Equal Partner, Aleph

The late 80's and early 90's played a pivotal role in the forming of the Israeli tech scene as we know it today, producing companies like Checkpoint, Waze, Wix, Mobileye, Viber and billions of dollars in fundraising and exits. The people who would later build that industry were in anywhere from elementary school to

high school, and their paths included some of the best hacking stories of the time (certainly in the eyes of the locals). The combination of extremely expensive Internet and international dial system, non-existent legal enforcement and a lagging national phone company could not prevent dozens of hungry-for-knowledge kids from teaching themselves the dark arts of reversing, hacking, cracking, phreaking and even carding. The world looked completely different back then and we have some great stories for you. We will cover the evolution of the many-years-later-to-be-named-Cyber community, including personal stories from nearly all categories. Come listen how the Israeli Cyber "empire" was born, 25 years ago, from the perspectives of 2:401/100 and 2:401/100.1.

PEIMA (PROBABILITY ENGINE TO IDENTIFY MALICIOUS ACTIVITY): USING POWER LAWS TO ADDRESS DENIAL OF SERVICE ATTACKS

Sunday at 10:20 in Track 2
20 minutes | Art of Defense, Demo, Tool

Redezem, Hacker

Denial of service. It requires a low level of resources and knowledge, it is very easy to deploy, it is very common and it is remarkable how effective it is overall. PEIMA is a brand new method of client side malicious activity detection based on mathematical laws, usually used in finance, text retrieval and social media analysis, that is fast, accurate, and capable of determining when denial of service attacks start and stop without flagging legitimate heavy interest in your server erroneously. However, denial of service attacks aren't the only type of anomalous activity you can look at with PEIMA. Learn what kinds of unusual identifying metrics you can get out of your network and users to help detect intrusions and, ultimately, defend your assets.

PRESENTATIONS

AN ACE UP THE SLEEVE: DESIGNING ACTIVE DIRECTORY DACL BACKDOORS

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

Andy Robbins, Red Team Lead
Will Schroeder, Offensive Engineer

Active Directory (AD) object discretionary access control lists (DACLS) are an untapped offensive landscape, often overlooked by attackers and defenders alike. The control relationships between AD objects align perfectly with the “attackers think in graphs” philosophy and expose an entire class of previously unseen control edges, dramatically expanding the number of paths to complete domain compromise.

While DACL misconfigurations can provide numerous paths that facilitate elevation of domain rights, they also present a unique chance to covertly deploy Active Directory persistence. It’s often difficult to determine whether a specific AD DACL misconfiguration was set intentionally or implemented by accident. This makes Active Directory DACL backdoors an excellent persistence opportunity: minimal forensic footprint, and maximum plausible deniability.

This talk will cover Active Directory DACLS in depth, our “misconfiguration taxonomy”, and enumeration/analysis with BloodHound’s newly released feature set. We will cover the abuse of AD DACL misconfigurations for the purpose of domain rights elevation, including common misconfigurations encountered in the wild. We will then cover methods to design AD DACL backdoors, including ways to evade current detections, and will conclude with defensive mitigation/detection techniques for everything described.

USING GPS SPOOFING TO CONTROL TIME

Friday at 14:00 in 101 Track
45 minutes | Tool

David “Karit” Robinson, Security Consultant, ZX Security

GPS is central to a lot of the systems we deal with on a day-to-day basis. Be it Uber, Tinder, or aviation systems, all of them rely on GPS signals to receive their location and/or time.

GPS Spoofing is now a valid attack vector and can be done with minimal effort and cost. This raises some concerns when GPS is depended upon by safety of life applications. This presentation will look at the process for GPS and NMEA (the serial format that GPS receivers output) spoofing, how to detect the spoofing attacks and ways to manipulate the time on GPS synced NTP servers. We will also explore the implications when the accuracy of the time on your server can no longer be guaranteed.

WIPING OUT CSRF

Thursday at 13:00 in 101 Track 2
45 minutes | Art of Defense, Demo

Joe Rozner, Senior Software Security Engineer, Prevoty

CSRF remains an elusive problem due to legacy code, legacy frameworks, and developers not understanding the problem or how to protect against it. Wiping out CSRF introduces primitives and strategies for building solutions to CSRF that can be bolted on to any http application where http requests and responses can be intercepted, inspected, and modified. Modern frameworks have done a great job at providing solutions to the CSRF problem that automatically integrate into the application and solve most of the conditions. However, many existing apps and new apps that don’t take advantage of these frameworks or use them incorrectly are still plagued with this problem. Wiping out CSRF will provide an in depth overview of the various reasons that CSRF occurs and provide payload examples to target those specific issues and variations. We’ll see live demos of these attacks and the protections against them. Next we’ll look at how to compose these primitives into a complete solution capable of solving most cases of CSRF explaining the limits and how to layer them to address potential short comings.

Finally we’ll finish by looking at Same Site Cookies, a new extension to cookies that could be the final nail in the coffin, and see how to use the prior solution as a graceful degradation for user agents that don’t support it yet.

THE BLACK ART OF WIRELESS POST EXPLOITATION

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

Gabriel “solstice” Ryan, Gotham Digital Science

Most forms of WPA2-EAP have been broken for nearly a decade. EAP-TLS and EAP-PEAP have long been susceptible to evil twin attacks, yet most enterprise organizations still rely on these technologies to secure their wireless infrastructure. The reason for this is that the secure alternative, EAP-TLS, is notoriously arduous to implement. To compensate for the weak perimeter security provided by EAP-TLS and EAP-PEAP, many organizations use port based NAC appliances to prevent attackers from pivoting further into the network after the wireless has been breached. This solution is thought to provide an acceptable balance between security and accessibility. The problem with this approach is that it assumes that EAP is exclusively a perimeter defense mechanism. In this presentation, we will present a novel type of rogue access point attack that can be used to bypass port-based access control mechanisms in wireless networks. In doing so, we will challenge the assumption that reactive approaches to wireless security are an acceptable alternative to strong physical layer protections such as WPA2-EAP using EAP-TLS.

TAKING WINDOWS 10 KERNEL EXPLOITATION TO THE NEXT LEVEL - LEVERAGING WRITE-WHAT-WHERE VULNERABILITIES IN CREATORS UPDATE

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

Morten Schenk, Security Advisor, Improsec

Since the release of Windows 10 and especially in the Anniversary and Creators Updates, Microsoft has continued to introduce exploit mitigations to the Windows kernel. These include full scale KASLR and blocking kernel pointer leaks.

This presentation picks up the mantle and reviews the powerful read and write kernel primitives that can still be leveraged despite the most recent hardening mitigations. The presented techniques include abusing the kernel-mode Window and Bitmap objects, which Microsoft has attempted to lock down several times. Doing so will present a generic approach to leveraging write-what-where vulnerabilities.

A stable and precise kernel exploit must be able to overcome KASLR, most often using kernel driver leaks. I will disclose several previously unknown KASLR bypasses in Windows 10 Creators Update. Obtaining kernel-mode code execution on Windows has become more difficult with the randomization of Page Table entries. I will show how a generic de-randomization of the Page Table entries can be performed through dynamic reverse engineering. Additionally, I will present an entirely different method which makes the usage of Page Table entries obsolete. This method allocates an arbitrary size piece of executable kernel pool memory and transfers code execution to it through hijacked system calls.

SOCIAL ENGINEERING THE NEWS

Standby Speaker
45 minutes

Michael Schrenk

It might be called “fake news” but at it’s heart, it’s the latest wave of social engineering. This apolitical talk explores the similarities between traditional social engineering and today’s “fake news”. During this talk, Michael Schrenk

will show how social engineers use OPSEC (Operations Security) to plan a successful social attack. Additionally, you’ll also learn the about the economics of “fake news”, who’s making the money, and how much, and how information is weaponized. This talk will also reveal that the news has been socialized for a long time, and that socially engineered news lead to the start of the Spanish American War. We’ll also explore techniques to guard against social engineering in general, and specifically in the media.

TOTAL RECALL: IMPLANTING PASSWORDS IN COGNITIVE MEMORY

Sunday at 11:00 in 101 Track
45 minutes

Tess Schrodinger

What is cognitive memory? How can you “implant” a password into it? Is this truly secure? Curiosity around these questions prompted exploration of the research and concepts surrounding the idea of making the authentication process more secure by implanting passwords into an individual’s memory. The result? The idea is that you are not able to reveal your credentials under duress but you are still able to authenticate to a system. We will begin with an understanding of cognitive memory. Implicit versus explicit memory will be defined. The concepts of the subconscious, unconscious, and consciousness will be addressed. The stages of memory pertaining to encoding, storage and retrieval as well as the limitations of human memory along with serial interception sequence learning training will round out our build up to the current research and experimentation being done with the proposal to implant passwords into an individual’s cognitive memory.

OPEN SOURCE SAFE CRACKING ROBOTS - COMBINATIONS UNDER 1 HOUR! (IS IT BAIT? DAMN STRAIGHT IT IS.)

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

Nathan Seidle, Founder, SparkFun Electronics

We’ve built a \$200 open source robot that cracks combination safes using a mixture of measuring techniques and set testing to reduce crack times

to under an hour. By using a motor with a high count encoder we can take measurements of the internal bits of a combination safe while it remains closed. These measurements expose one of the digits of the combination needed to open a standard fire safe. Additionally, ‘set testing’ is a new method we created to decrease the time between combination attempts. With some 3D printing, Arduino, and some strong magnets we can crack almost any fire safe. Come checkout the live cracking demo during the talk!

MAN IN THE NFC

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

Haoqi Shan, Wireless security researcher

Jian Yuan, Wireless security researcher

NFC (Near Field Communication) technology is widely used in security, bank, payment and personal information exchange fields now, which is highly well-developed. Corresponding, the attacking methods against NFC are also emerged in endlessly. To solve this problem, we built a hardware tool which we called “UniProxy”. This tool contains two self-modified high frequency card readers and two radio transmitters, which is a master-slave way. The master part can help people easily and successfully read almost all ISO 14443A type cards, (no matter what kind of this card is, bank card, ID card, Passport, access card, or whatever. No matter what security protocol this card uses, as long as it meets the ISO 14443A standard) meanwhile replaying this card to corresponding legal card reader via slave part to achieve our “evil” goals. The master and slave communicate with radio transmitters and can be apart between 50 - 200 meters.

PRESENTATIONS

DRIVING DOWN THE RABBIT HOLE

Saturday at 12:00 in 101 Track
45 minutes | Demo

Mickey Shkatov, Security Researcher, McAfee.

Jesse Michael, Security Researcher, McAfee.

Oleksandr Bazhaniuk, Security Researcher

Over the past few years, cars and automotive systems have gained increasing attention as cyber-attack targets. Cars are expensive. Breaking cars can cost a lot. So how can we find vulnerabilities in a car with no budget? We'll take you with us on a journey from zero car security validation experience through the discovery and disclosure of multiple remotely-exploitable automotive vulnerabilities. Along the way, we'll visit a wrecking yard, reassemble (most) of a 2015 Nissan Leaf in our lab, discuss how we picked our battles, fought them, and won. During our talk, we'll examine the details of three different classes of vulnerabilities we found in this vehicle, how they can be exploited, and the potential ramifications to the owner of their real-world exploitation. We'll also discuss the broader scope of the vulnerabilities discovered, how they extend beyond just this specific vehicle, and what the industry can do better to prevent these types of problems in the future.

HERE TO STAY: GAINING PERSISTENCY BY ABUSING ADVANCED AUTHENTICATION MECHANISMS

Saturday at 17:00 in 101 Track
45 minutes | Demo

Marina Simakov, Security researcher, Microsoft

Igal Gofman, Security researcher, Microsoft

Credentials have always served as a favorite target for advanced attackers, since these allow to efficiently traverse a network, without using any exploits.

Moreover, compromising the network might not be sufficient, as attackers strive to

obtain persistency, which requires the use of advanced techniques to evade the security mechanisms installed along the way.

One of the challenges adversaries must face is: How to create threats that will continuously evade security mechanisms, and even if detected, ensure that control of the environment can be easily regained?

In this talk, we briefly discuss some of the past techniques for gaining persistency in a network (using local accounts, GPOs, skeleton key, etc.) and why they are insufficient nowadays.

Followed by a comprehensive analysis of lesser known mechanisms to achieve persistency, using non-mainstream methods (such as object manipulation, Kerberos delegation, etc.).

Finally, we show how defenders can secure their environment against such threats.

ABUSING WEBHOOKS FOR COMMAND AND CONTROL

Saturday at 11:20 in 101 Track
20 minutes | Demo, Tool

Dimitry Snezhkov, Security Consultant, X-Force Red, IBM

You are on the inside of the perimeter. And maybe you want to exfiltrate data, download a tool, or execute commands on your command and control server (C2). Problem is - the first leg of connectivity to your C2 is denied. Your DNS and ICMP traffic is being monitored. Access to your cloud drives is restricted. You've implemented domain fronting for your C2 only to discover it is ranked low by the content proxy, which is only allowing access to a handful of business related websites on the outside.

We have all been there, seeing frustrating proxy denies or triggering security alarms making our presence known. Having more choices when it comes to outbound network connectivity helps. In this talk we'll present a technique to establish such connectivity with the help of HTTP callbacks (webhooks). We will walk you through what webhooks are, how they are used by organizations. We will then discuss how you can use approved sites as brokers of your communication, perform data transfers, establish almost realtime asynchronous command execution, and even

create a command-and-control communication over them, bypassing strict defensive proxies, and even avoiding attribution.

Finally, we'll release the tool that will use the concept of a broker website to work with the external C2 using webhooks.

PHONE SYSTEM TESTING AND OTHER FUN TRICKS

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

"Snide" Owen, Hacker

Phone systems have been long forgotten in favor of more modern technology. The phreakers of the past left us a wealth of information, however while moving forward the environments as a whole have become more complex. As a result they are often forgotten, side tracked or neglected to be thoroughly tested. We'll cover the VoIP landscape, how to test the various components while focussing on PBX and IVR testing. The security issues that may be encountered are mapped to the relative OWASP category for familiarity. Moving on I'll demonstrate other fun ways that you can utilize a PBX within your future offensive endeavours.

HACKING TRAVEL ROUTERS LIKE IT'S 1999

Friday at 10:20 in Track 2
20 minutes | Demo, Exploit

Mikhail Sosonkin, Security Researcher, Synack Inc.

Digital nomads are a growing community and they need internet safety just like anyone else. Trusted security researchers have warned about the dangers of traveling through Airbnb's. Heeding their advice, I purchased a HooToo TM06 travel router to create my own little enclave while I bounce the globe. Being a researcher myself, I did some double checking.

So, I started fuzzing and reverse engineering. While the TM06 is a cute and versatile little device - protection against network threats, it is not. In this talk, I will take you on my journey revealing my methodology for discovering and exploiting two memory corruption vulnerabilities. The vulnerabilities are severe and while they've been reported to the vendor, they are very revealing data points about the security state of such devices. While the device employs some

exploitation mitigations, there are many missing. I will be showing how I was able to bypass them and what mitigations should've been employed, such as NX-Stack/Heap, canaries, etc, to prevent me from gaining arbitrary shellcode execution.

If you're interested in security of embedded/IoT systems, travel routers or just good old fashioned MIPS hacking, then this talk is for you!

GENETIC DISEASES TO GUIDE DIGITAL HACKS OF THE HUMAN GENOME: HOW THE CANCER MOONSHOT PROGRAM WILL ENABLE ALMOST ANYONE TO CRASH THE OPERATING SYSTEM THAT RUNS YOU OR TO END CIVILIZATION...

Sunday at 12:00 in Track 4
45 minutes

John Sotos, Chief Medical Officer, Intel Corporation

The human genome is, fundamentally, a complex open-source digital operating system (and set of application programs) built on the digital molecules DNA and RNA.

The genome has thousands of publicly documented, unpatchable security vulnerabilities, previously called "genetic diseases." Because emerging DNA/RNA technologies, including CRISPR-Cas9 and especially those arising from the Cancer Moonshot program, will create straightforward methods to digitally reprogram the genome in free-living humans, malicious exploitation of genomic vulnerabilities will soon be possible on a wide scale.

This presentation shows the breathtaking potential for such hacks, most notably the exquisite targeting precision that the genome supports — in effect, population, and time — spanning annoyance to organized crime to civilization-ending pandemics far worse than Ebola.

Because humans are poor at responding to less-than-immediate threats, and because there is no marketplace demand for defensive technologies on the DNA/RNA platform, the hacker community has an important role to play in devising thought-experiments to convince policy makers

to initiate defensive works, before offensive hacks can be deployed in the wild. Hackers can literally save the world... from ourselves.

EXPLOITING CONTINUOUS INTEGRATION (CI) AND AUTOMATED BUILD SYSTEMS

Sunday at 11:00 in Track 3
45 minutes | Demo, Tool, Exploit

spaceB0x, Sr. Security Engineer at LeanKit Inc.

Continuous Integration (CI) systems and similar architecture has taken new direction, especially in the last few years. Automating code builds, tests, and deployments is helping hordes of developers release code, and is saving companies a great amount of time and resources. But at what cost? The sudden and strong demand for these systems have created some widely adopted practices that have large security implications, especially if these systems are hosted internally. I have developed a tool that will help automate some offensive testing against certain popular CI build systems. There has been a large adoption of initiating these builds through web hooks of various kinds, especially changes to public facing code repositories. I will start with a brief overview of some of the more popular CI tools and how they are being used in many organizations. This is good information for understanding, at a high level, the purpose of these systems as well as some security benefits that they can provide. From there we will dive into specific examples of how these different CI implementations have created vulnerabilities (in one case to a CI vendor themselves). Last we will explore the tool, its purpose, and a demonstration of its use. This tool takes advantage of the configurations of various components of the build chain to look for vulnerabilities. It then has the capability to exploit, persist access, command and control vulnerable build containers. Most of the demonstration will revolve around specific CI products and repositories, however the concepts are applicable across most build systems. The goal here is to encourage further exploration of these exploitation concepts. The tool is built "modularly" to facilitate this. If you are new to

CI and automated build systems, or if you have been doing it for years, this talk and tool will help you to better secure your architecture.

BREAKING WIND: ADVENTURES IN HACKING WIND FARM CONTROL NETWORKS

Saturday at 10:20 in 101 Track
20 minutes

Jason Staggs, Security Researcher at the University of Tulsa

Wind farms are becoming a leading source for renewable energy. The increased reliance on wind energy makes wind farm control systems attractive targets for attackers. This talk explains how wind farm control networks work and how they can be attacked in order to negatively influence wind farm operations (e.g., wind turbine hijacking). Specifically, implementations of the IEC 61400-25 family of communications protocols are investigated (i.e., OPC XML-DA). This research is based on an empirical study of a variety of U.S. based wind farms conducted over a two year period. We explain how these security assessments reveal that wind farm vendor design and implementation flaws have left wind turbine programmable automation controllers and OPC servers vulnerable to attack. Additionally, proof-of-concept attack tools are developed in order to exploit wind farm control network design and implementation vulnerabilities.

HACKING THE CLOUD

Thursday at 14:00 in 101 Track
45 minutes | Demo

Gerald Steere, Cloud Wrecker, Microsoft

Sean Metcalf, CTO, Trimarc

You know the ins and outs of pivoting through your target's domains. You've had the KRBTGT hash for months and laid everything bare. Or have you?

More targets today have some or all of their infrastructure in the cloud. Do you know how to follow once the path leads there? Red teams and penetration testers need to think beyond the traditional network boundaries and follow the data and services they are

PRESENTATIONS

after. This talk will focus on how to take domain access and leverage internal access as a ticket to your target's cloud deployments.

We will also discuss round trip flights from cloud to on-premises targets and what authorizations are required to access your target's cloud deployments. While this talk is largely focused on Microsoft Azure implementations, the concepts can be applied to most cloud providers.

RAGE AGAINST THE WEAPONIZED AI PROPAGANDA MACHINE

Friday at 11:00 in 101 Track
45 minutes | 0025

Suggy (AKA Chris Sumner),
Researcher, The Online Privacy
Foundation

Psychographic targeting and the so called "Weaponized AI Propaganda Machine" have been blamed for swaying public opinion in recent political campaigns. But how effective are they? Why are people so divided on certain topics? And what influences their views? This talk presents the results of five studies exploring each of these questions. The studies examined authoritarianism, threat perception, personality-targeted advertising and biases in relation to support for communication surveillance as a counter-terrorism strategy. We found that people with an authoritarian disposition were more likely to be supportive of surveillance, but that those who are less authoritarian became increasingly supportive of such surveillance the greater they perceived the threat of terrorism. Using psychographic targeting we reached Facebook audiences with significantly different views on surveillance and demonstrated how tailoring pro and anti-surveillance ads based on authoritarianism affected return on marketing investment. Finally, we show how debunking propaganda faces big challenges as biases severely limit a person's ability to interpret evidence which runs contrary to their beliefs. The results illustrate the effectiveness of psychographic targeting and the ease with which individuals' inherent differences and biases can be exploited.

FOROSITY: A DECOMPILE FOR BLOCKCHAIN-BASED SMART CONTRACTS BYTECODE

Thursday at 12:00 in 101 Track
45 minutes | Demo, Tool

Matt Suiche, Founder, Comae
Technologies

Ethereum is gaining a significant popularity in the blockchain community, mainly due to fact that it is design in a way that enables developers to write decentralized applications (Dapps) and smart-contract using blockchain technology.

Ethereum blockchain is a consensus-based globally executed virtual machine, also referred as Ethereum Virtual Machine (EVM) by implemented its own micro-kernel supporting a handful number of instructions, its own stack, memory and storage. This enables the radical new concept of distributed applications.

Contracts live on the blockchain in an Ethereum-specific binary format (EVM bytecode). However, contracts are typically written in some high-level language such as Solidity and then compiled into byte code to be uploaded on the blockchain. Solidity is a contract-oriented, high-level language whose syntax is similar to that of JavaScript. This new paradigm of applications opens the door to many possibilities and opportunities. Blockchain is often referred as secure by design, but now that blockchains can embed applications this raise multiple questions regarding architecture, design, attack vectors and patch deployments.

As we, reverse engineers, know having access to source code is often a luxury. Hence, the need for an open-source tool like Porosity: decompiler for EVM bytecode into readable Solidity-syntax contracts - to enable static and dynamic analysis of compiled contracts.

GAME OF CHROMES: OWNING THE WEB WITH ZOMBIE CHROME EXTENSIONS

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

Tomer Cohen, R&D Security Team
Leader, Wix.com

On April 16 2016, an army of bots stormed upon Wix servers, creating new accounts and publishing shady websites in mass. The attack was carried by a malicious Chrome extension, installed on tens of thousands of devices, sending HTTP requests simultaneously. This "Extension Bot" has used Wix websites platform and Facebook messaging service, to distribute itself among users. Two months later, same attackers strike again. This time they used infectious notifications, popping up on Facebook and leading to a malicious Windows-runnable JSE file. Upon clicking, the file ran and installed a Chrome extension on the victim's browser. Then the extension used Facebook messaging once again to pass itself on to more victims.

Analyzing these attacks, we were amazed by the highly elusive nature of these bots, especially when it comes to bypassing web-based bot-detection systems. This shouldn't be surprising, since legit browser extensions are supposed to send Facebook messages, create Wix websites, or in fact perform any action on behalf of the user.

On the other hand, smuggling a malicious extension into Google Web Store and distributing it among victims efficiently, like these attackers did, is let's say - not a stroll in the park. But don't worry, there are other options.

Recently, several popular Chrome extensions were found to be vulnerable to XSS. Yep, the same old XSS every rookie finds in so many web applications. So browser extensions suffer from it too, and sadly, in their case it can be much deadlier than in regular websites. One noticeable example is the Adobe Acrobat Chrome extension, which was silently installed on January 10 by Adobe, on an insane number of 30 million devices. A DOM-based XSS vulnerability in the extension (found by Google Project Zero) allowed an attacker to craft a content that would run Javascript as the extension.

In this talk I will show how such a flaw leads to full and permanent control over the victim's browser, turning the extension into zombie. Additionally, Shedding more light on the 2016 attacks on Wix and Facebook described in the beginning, I will demonstrate how an attacker can use similar techniques to distribute her malicious payload efficiently on to new victims, through popular social platforms - creating the web's most powerful botnet ever.

WHEN PRIVACY GOES POOF! WHY IT'S GONE AND NEVER COMING BACK

Saturday at 12:00 in Track 2
45 minutes | 0025

Richard Thieme a.k.a. neuralcowboy

"Get over it!" as Scott McNeely said - unhelpfully. Only if we understand why it is gone and not coming back do we have a shot at rethinking what privacy means in a new context. Thieme goes deep and wide as he rethinks the place of privacy in the new social/cultural context and challenges contemporary discussions to stop using 20th century frames. Pictures don't fit those frames, including pictures of "ourselves."

We have always known we were cells in a body, but we emphasized "cell-ness". Now we have to emphasize "body-ness" and see ourselves differently. What we see depends on the level of abstraction at which we look. The boundaries we imagine around identities, psyches, private internal spaces," are violated in both directions, going in and going out, by data that, when aggregated, constitutes "us". We are known by others more deeply in recombination from metadata than we know ourselves. We are not who we think we are.

To understand privacy - even what we mean by "individuals" who want it - requires a contrary opinion. Privacy is honored in lip service, but not in the marketplace, where it is violated every day. To confront the challenges of technological change, we have to know what is happening to "us" so we can re-imagine what we mean by privacy, security, and identity. We can't say what we can't think. We need new language to grasp our own new "human nature" that has been reconstituted from elements like orange juice.

PRESENTATIONS

The weakest link in discussions of privacy is the definition of privacy, and the definition of privacy is not what we think. Buddhists call enlightenment a "nightmare in daylight", yet it is enlightenment still, and that kind of clarity is the goal of this presentation.

MS JUST GAVE THE BLUE TEAM TACTICAL NUKES (AND HOW RED TEAMS NEED TO ADAPT)

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

Chris Thompson, Red Team Ops Lead,
IBM X-Force Red

Windows Defender Advanced Threat Protection will soon be available for all Blue Teams to utilize within Windows 10 Enterprise, which includes detection of post breach tools, tactics and techniques commonly used by Red Teams, as well as behavior analytics. Combined with Microsoft Advanced Threat Analytics for user behavior analytics across the Domain, Red Teamers will soon face a significantly more challenging time maintaining stealth while performing internal recon, lateral movement, and privilege escalation in Windows 10/Active Directory environments.

This talk highlights challenges to red teams posed by Microsoft's new tools based on common hacking tools/techniques, and covers techniques which can be used to bypass, disable, or avoid high severity alerts within Windows Defender ATP and Microsoft ATA, as well as TTP used against mature organizations that may have additional controls in place such as Event Log Forwarding and Sysmon.

DOOMED POINT OF SALE SYSTEMS

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

trixr4skids, Security Engineer

In response to public security breaches many retailers have begun efforts to minimize or completely prevent the transmission of unencrypted credit card data through their store networks and point of sale systems. While this is definitely a great improvement over the previous state of affairs; it places the security of transactions squarely in the hands of credit card terminals purchased from third

party vendors. These terminals have a security posture that is often not well understood by the retail chains purchasing them. To better understand if the trust placed in these devices is warranted, the attack surface and hardening of a commonly deployed credit card terminal series is reviewed and a discussion of reverse engineered security APIs is presented. Despite the reduced attack surface of the terminals and hardened configuration, attacks that allow recovery of magstripe track data and PIN codes are demonstrated to be possible.

A NEW ERA OF SSRF - EXPLOITING URL PARSER IN TRENDING PROGRAMMING LANGUAGES!

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

Orange Tsai, Security Consultant
from DEVCORE

We propose a new exploit technique that brings a whole-new attack surface to bypass SSRF (Server Side Request Forgery) protections. This is a very general attack approach, in which we used in combination with our own fuzzing tool to discover many Odays in built-in libraries of very widely-used programming languages, including Python, PHP, Perl, Ruby, Java, JavaScript, Wget and cURL. The root cause of the problem lies in the inconsistency of URL parsers and URL requesters.

Being a very fundamental problem that exists in built-in libraries, sophisticated web applications such as WordPress (27% of the Web), vBulletin, MyBB and GitHub can also suffer, and Odays have been discovered in them via this technique. This general technique can also adapt to various code contexts and lead to protocol smuggling and SSRF bypassing. Several scenarios will be demonstrated to illustrate how URL parsers can be exploited to bypass SSRF protection and achieve RCE (Remote Code Execution), which is the case in our GitHub Enterprise demo.

Understanding the basics of this technique, the audience won't be surprised to know that more than 20 vulnerabilities have been found in famous programming languages and web applications aforementioned via this technique.

PRESENTATIONS

A PICTURE IS WORTH A THOUSAND WORDS, LITERALLY: DEEP NEURAL NETWORKS FOR SOCIAL STEGO

Saturday at 13:00 in Track 4
45 minutes | Tool

Philip Tully, Principal Data Scientist, ZeroFOX

Michael T. Raggon, Chief Security Officer, AQ2 Secure

Images, videos and other digital media provide a convenient and expressive way to communicate through social networks. But such broadcastable and information-rich content provides ample illicit opportunity as well. Web-prevalent image files like JPEGs can be disguised with foreign data since they're perceivably robust to minor pixel and metadata alterations. Slipping a covert message into one of the billions of daily posted images may be possible, but to what extent can steganography be systematically automated and scaled?

To explore this, we first report the distorting side effects rendered upon images uploaded to popular social network servers, e.g. compression, resizing, format conversion, and metadata stripping. Then, we build a convolutional neural network that learns to reverse engineer these transformations by optimizing hidden data throughput capacity. From pre-uploaded and downloaded image files, the network learns to locate candidate metadata and pixels that are least modifiable during transit, allowing stored hidden payloads to be reliably recalled from newly presented images. Deep learning typically requires tons of training data to avoid over fitting. But data acquisition is trivial using social networks' free image hosting services, which feature bulk uploads and downloads of thousands of images at a time per album.

We show that hidden data can be predictably transmitted through social network images with high fidelity. Our results demonstrate that AI can hide data in plain sight, at large-scale, beyond human visual discernment, and despite third-party manipulation. Steganalysis and other defensive forensic countermeasures are notoriously difficult, and our exfiltration techniques highlight the growing threat posed by automated, AI-powered red teaming.

ARE ALL BSDS ARE CREATED EQUALLY? A SURVEY OF BSD KERNEL VULNERABILITIES.

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

Ilja van Sprundel, Director of penetration testing, IOActive

In this presentation I start off asking the question "How come there are only a handful of BSD security kernel bugs advisories released every year?" and then proceed to try and look at some data from several sources. It should come as no surprise that those sources are fairly limited and somewhat outdated.

The presentation then moves on to try and collect some data ourselves. This is done by actively investigating and auditing. Code review, fuzzing, runtime testing on all 3 major BSD distributions [NetBSD/OpenBSD/FreeBSD]. This is done by first investigating what would be good places where the bugs might be. Once determined, a detailed review is performed of these places. Samples and demos will be shown.

I end the presentation with some results and conclusions. I will list what the outcome was in terms of bugs found, and who -based on the data I now have- among the 3 main BSD distributions can be seen as the clear winner and loser. I will go into detail about the code quality observed and give some pointers on how to improve some code. Lastly I will try and answer the question I set out to answer ("How come there are only a handful of BSD security kernel bugs advisories released every year?").

THE LAST CTF TALK YOU'LL EVER NEED: AMA WITH 20 YEARS OF DEF CON CAPTURE-THE-FLAG ORGANIZERS

Thursday at 16:00 in 101 Track 2
105 minutes | Hacker History

Vulc@n, Difensiva Senior Engineer, DDTEK

Hawaii John, CTF organizer, Legit Business Syndicate

Chris Eagle, CTF organizer, DDTEK

Invisigoth, CTF organizer, Kenshoto

Caesar, CTF organizer, Ghetto Hackers

Myles, CTF organizer, Goon

Today there is practically a year-round CTF circuit, on which teams hone their skills, win prizes and attain stature. For many, the ultimate goal is to dominate in the utmost competition, DEF CON's CTF, and walk away with a coveted black badge. Capture-the-Flag (CTF) is one of DEF CON's oldest contests, dating back to DEF CON 4. Over the past decades, the perennial contest has matured into an annual event requiring months of preparation and nearly continuous dedication both of players and organizers. Organizers strive to make the events unique while taking extreme measures to prevent games from being gamed. Participants often have to cope with novel challenges while simultaneously demonstrating continued excellence in domains like reverse engineering, vulnerability discovery, exploitation, digital forensics, cryptography, and network security. In this session, we will present the evolution of DEF CON CTF, highlighting key points of advancement in the CTF culture - most of which broke new ground and are now present in other contests run around the world. Capitalizing on the multi-year tenure of recent DEF CON CTF organizers, we are able to concisely represent over 20 years of organizers on a single panel. Where else can you ask cross-generational questions about challenges of running CTF? Where else can you inquire about evolutionary design, and get answers from those that actually did it? Where else can you ask about hidden challenges, secrets, and CTF lore...from whom it originated?

The panelists represent over 20 years of DEF CON CTF organizers. Staples in the CTF community are present comprising of decades of experience in participating and organizing CTFs. On stage we have past organizers representing Legit BS, DDTEK, Kenshoto, Ghetto Hackers, and before - many of which also participated as part of top recurring teams such as Sk3wl of r00t, Ghetto Hackers, Samurai, and Team Awesome. Many also played some role (infrastructure, challenge author, announcer) in the Cyber Grand Challenge culminating last summer at DEF CON. They have received and distributed dozens of black badges. Panelists and the roles they represent for this panel: Hawaii John, Legit Business Syndicate; Chris Eagle, DDTEK; Invisigoth, Kenshoto; Caesar, Ghetto Hackers; Myles, Goon.

OFFENSIVE MALWARE ANALYSIS: DISSECTING OSX/FRUITFLY VIA A CUSTOM C&C SERVER

Friday at 10:20 in 101 Track
20 minutes | Demo, Tool

Patrick Wardle, Chief Security Researcher, Synack / Creator of Objective-See

Creating a custom command and control (C&C) server for someone else's malware has a myriad of benefits. If you can take over it a domain, you then may be able to fully hijack other hackers' infected hosts. A more prosaic benefit is expediting analysis. While hackers and governments may be more interested in the former, malware analysts can benefit from the later.

FruitFly, the first OS X/macOS malware of 2017, is a rather intriguing specimen. Selectively targeting biomedical research institutions, it is thought to have flown under the radar for many years. In this talk, we'll focus on the 'B' variant of FruitFly that even now, is only detected by a handful of security products.

We'll begin by analyzing the malware's dropper, an obfuscated perl script. As this language is rather archaic and uncommon in malware droppers, we'll discuss some debugging techniques and fully deconstruct the script.

While this dropper component also communicates with the C&C server and supports some basic commands, it drops a binary payload in order

to perform more complex actions. However, instead of fully reversing this piece of the malware, the talk will focus on an initial triage and show how this was sufficient for the creation of a custom C&C server. With such a server, we can easily coerce the malware to reveal it's full capabilities. For example, the malware invokes a handful of low-level mouse & graphics APIs, passing in a variety of dynamic parameters. Instead of spending hours reversing and debugging this complex code, via the C&C server, we can simply send it various commands and observe the effects.

Of course this approach hinges on the ability to closely observe the malware's actions. As such, we'll discuss macOS-specific tools that can monitor various events, and where necessary detail the creation of custom ones (e.g. a 'mouse sniffer' that locally observes and decodes commands sent from the malware to the OS, in order to control the mouse).

While some of this talk is FruitFly and/or macOS specific, conceptually it should broadly apply to analyzing other malware, even on other operating systems :)

DEATH BY 1000 INSTALLERS: ON MACOS, IT'S ALL BROKEN!

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

Patrick Wardle, Chief Security Researcher, Synack

Ever get an uneasy feeling when an installer asks for your password? Well, your gut was right! The majority of macOS installers & updaters are vulnerable to a wide range of priv-esc attacks.

It began with the discovery that Apple's OS updater could be abused to bypass SIP (CVE-2017-6974). Next, turns out Apple's core installer app may be subverted to load unsigned dylibs which may elevate privileges to root.

And what about 3rd-party installers? I looked at what's installed on my Mac, and ahhh, so many bugs!

Firewall, Little Snitch: EoP via race condition of insecure plistAnti-Virus, Sophos: EoP via hijack of binary component Browser, Google Chrome: EoP via script hijackVirtualization,

VMWare Fusion: EoP via race condition of insecure scriptIoT, DropCam: EoP via hijack of binary componentand more!

...and 3rd-party auto-update frameworks like Sparkle -yup vulnerable too!

Though root is great, we can't bypass SIP nor load unsigned kexts. However with root, I discovered one could now trigger a ring-0 heap-overflow that provides complete system control.

Though the talk will discuss a variety of discovery mechanisms, 0days, and macOS exploitation techniques, it won't be all doom & gloom. We'll end by discussing ways to perform authorized installs/upgrades that don't undermine system security."

IF YOU GIVE A MOUSE A MICROCHIP... IT WILL EXECUTE A PAYLOAD AND CHEAT AT YOUR HIGH-STAKES VIDEO GAME TOURNAMENT

Saturday at 11:00 in Track 3
45 minutes | Demo

skud (Mark Williams), Embedded Software Engineer

Sky (Rob Stanley), Security Software Engineer, Lead

The International, a recent esports tournament, had a 20 million dollar prize pool with over five million people tuned in to the final match. The high stakes environment at tournaments creates an incentive for players to cheat for a competitive advantage. Cheaters are always finding new ways to modify software, from attempting to sneak executables in on flash drives, to using cheats stored in Steam's online workshop which bypasses IP restrictions.

This presentation describes how one can circumvent existing security controls to sneak a payload (game cheat) onto a target computer. Esports tournaments typically allow players to provide their own mouse and keyboard, as these players prefer to use specific devices or may be obligated to use a sponsor branded device. These "simple" USB input devices can still be used to execute complex commands on a computer via the USB Human Interface Device (HID) protocol.

Our attack vector is a mouse with an ARM Cortex M series processor. The microcontroller stores

PRESENTATIONS

custom user profiles in flash memory, allowing the mouse to retain user settings between multiple computers. We modify the device's firmware to execute a payload delivery program, stored in free space in flash memory, before returning the mouse to its original functionality. Retaining original functionality allows the mouse to be used discreetly, as it is an "expected" device at these tournaments. This concept applies to any USB device that uses this processor, and does not require obvious physical modifications.

This delivery method has tradeoffs. Our exploit is observable, as windows are created and in focus during payload delivery. The advantage to this approach is that it bypasses other security measures that are commonly in place, such as filtered internet traffic and disabled USB mass storage.

SEE NO EVIL, HEAR NO EVIL: HACKING INVISIBLY AND SILENTLY WITH LIGHT AND SOUND

Thursday at 14:00 in 101 Track 2
45 minutes | Demo, Tool

Matt Wixey, Senior Associate, PwC

Traditional techniques for C2 channels, exfiltration, surveillance, and exploitation are often frustrated by the growing sophistication and prevalence of security protections, monitoring solutions, and controls. Whilst all is definitely not lost, from an attacker's perspective - we constantly see examples of attackers creatively bypassing such protections - it is always beneficial to have more weapons in one's arsenal, particularly when coming up against heavily-defended networks and highly-secured environments.

This talk demonstrates a number of techniques and attacks which leverage light and/or sound, using off-the-shelf hardware. It covers everything from C2 channels and exfiltration using light and near-ultrasonic sound, to disabling and disrupting motion detectors; from laser microphones, to repelling drones; from trolling friends, to jamming speech and demotivating malware analysts.

This talk not only provides attendees with a new suite of techniques and methodologies to consider when coming up against a

well-defended target, but also demonstrates, in a hopefully fun and practical way, how these techniques work, their advantages, disadvantages, and possible future developments. It also gives details of real case studies where some of these techniques have been used, and provides defenders with realistic methods for the mitigation of these attacks.

Finally, the talk covers some ideas for future research in this area.

ASSEMBLY LANGUAGE IS TOO HIGH LEVEL

Friday at 15:00 in 101 Track
45 minutes | Demo, Tool, Exploit

XlogicX, Machine Hacker

Do you have a collection of vulnerable programs that you have not yet been able to exploit? There may yet still be hope. This talk will show you how to look deeper (lower level). If you've ever heard experts say how x86 assembly language is just a one-to-one relationship to its machine-code, then we need to have a talk. This is that talk; gruesome detail on how an assembly instruction can have multiple valid representations in machine-code and vice versa. You can also just take my word for it, ignore the details like a bro, and use the tool that will be released for this talk: the Interactive Redundant Assembler (irasm). You can just copy the alternate machine code from the tool and use it in other tools like mona, use it to give yourself more options for self-modifying code, fork Hydan (stego) and give it more variety, or to create peace on earth.

THERE'S NO PLACE LIKE 127.0.0.1 - ACHIEVING RELIABLE DNS REBINDING IN MODERN BROWSERS

Thursday at 10:00 in 101 Track
45 minutes | Demo, Tool, Exploit

Luke Young, Senior Information Security Engineer, LinkedIn

Most people lock their doors at night, however if you walk into someone's home you likely won't find every piece of furniture bolted to the floor as well. We trust that if someone is inside our home they are supposed to be there. Unfortunately many developers treat local networks just the same, assuming all internal HTTP traffic is trusted, however this is not always

the case. They incorrectly assume that their services will be protected by the same-origin policy in browsers, rather than implementing proper authentication mechanisms. By abusing this implicit trust we can gain access to confidential data and internal services which are not intended to be publicly accessible.

I will demonstrate that this is a poor security control and can be trivially bypassed via an older technique, DNS rebinding. The talk will cover how DNS rebinding works, the mitigations imposed by modern browsers and networks, and how each mitigation can be bypassed. I will discuss the notorious unreliability of DNS rebinding attacks that causes many developers to ignore the issue and how to overcome this unreliability.

Finally, I will examine a variety of popular services and tools to understand how they are affected by DNS rebinding. I will be releasing a tool that allows researchers to automate DNS rebinding attacks, the associated mitigation bypasses and generate drop-dead simple proof-of-concept exploits. I will demonstrate this tool by developing exploits for each vulnerable service, ending the talk by exploiting a vulnerable service to obtain remote-code execution, live.

25 YEARS OF PROGRAM ANALYSIS

Sunday at 15:00 in 101 Track
45 minutes | Hacker History, Demo

Zardus (Yan Shoshitaishvili), Assistant Professor, Arizona State University

Last year, DARPA hosted the Cyber Grand Challenge, the culmination of humanity's research into autonomous detection, exploitation, and mitigation of software vulnerabilities. Imagine the CGC from the outside: huge racks of servers battling it out on stage, throwing exploit after exploit at each other while humans watch helplessly from the sidelines. But that vantage point misses the program analysis methods used, the subtle trade-offs made, and the actual capabilities of these systems. It also misses why, outside of the controlled CGC environment, most automated techniques don't quite scale to the analysis of real-world software!

This talk will provide a better perspective. On the 25th anniversary of DEFCON, we will go through these last 25 years of program analysis.

We'll learn about the different disciplines of program analysis (and learn strange terms such as static, dynamic, symbolic, and abstract), understand the strength and drawbacks of each, and see if, and to what extent, they are used in the course of actual vulnerability analysis.

Did you know that every finalist system in the Cyber Grand Challenge used a combination of dynamic analysis and symbolic execution to find vulnerabilities, but used static analysis to patch them? Why is that? Did you know that, to make the contest feasible for modern program analysis techniques, the CGC enforced a drastically-simplified OS model? What does this mean for you, if you want to use program analysis while finding vulns and collecting bug bounties? Come to this talk, become an expert, and go on to contribute to the future of program analysis!

CITL AND THE DIGITAL STANDARD - A YEAR LATER

Friday at 12:00 in 101 Track
45 minutes | Art of Defense

Sarah Zatkos, Chief Scientist, Cyber ITL

A year ago, Mudge and I introduced the non-profit Cyber ITL at DEF CON and its approach to automated software safety analysis. Now, we'll be covering highlights from the past year's research findings, including our in-depth analysis of several different operating systems, browsers, and IoT products.

Parts of our methodologies have now been adopted by Consumer Reports and rolled into their Digital Standard for evaluating safety, security, and privacy, in a range of consumer devices. The standard defines important consumer values that must be addressed in product development, with the goal of enabling consumer organizations to test, evaluate, and report on whether new products protect consumer security, safety, and privacy.

ALL YOUR THINGS ARE BELONG TO US

Saturday at 11:20 in Track 4
75 minutes | Demo, Exploit

Zenofex, Hacker
0x00string, Hacker
CJ_000, Hacker
Maximus64, Hacker

Get out your rollerblades, plug in your camo keyboard, and fire up your BLT drive. It's 25 years later and we're still hacking the planet. The Exploitee.rs are back with new Oday, new exploits and more fun. Celebrating a quarter century of DEF CON the best way we know how: hacking everything!

Our presentation will showcase vulnerabilities discovered during our research into thousands of dollars of IoT gear performed exclusively for DEF CON. We will be releasing all the vulnerabilities during the presentation as Odays to give attendees the ability to go home and unlock their hardware prior to patches being released. As always, to give back to the community that has given us so much, we will be handing out free hardware during the presentation so you can hack all the things too! Come party with us while we make "All Your Things Are Belong To Us."

MACOS/IOS KERNEL DEBUGGING AND HEAP FENG SHUI

Friday at 10:00 in 101 Track
20 minutes

Min(Spark) Zheng, Security Expert @ Alibaba Inc. Ph.D of CUHK.
Xiangyu Liu, Security Engineer @ Alibaba Inc. Ph.D of CUHK.

Kernel bug is always very difficult to reproduce and may lead to the entire system panic and restart. In practice, kernel debugging is the only way to analyze panic scenes. However, implementing such a technique in real world is not an easy task since kernel code cannot be executed in the debugger, thus is hard to be tracked. Luckily, macOS has provided a very powerful kernel debugging mechanism, KDK (Kernel Development Kit), to assist people to analyze and develop kernel exploits. While for iOS, although there is no official kernel debugger, it is also possible for us to achieve kernel debugging by leveraging some tricks.

In this talk, we will share some kernel debugging techniques and their corresponding tricks on the latest iOS/macOS. In addition, we will also introduce the new kernel heap mitigation mechanisms on iOS 10/macOS 10.12 and two heap feng shui techniques to bypass them. Finally, we will demonstrate how to debug a concrete kernel heap overflow bug and then leverage our new heap feng shui techniques to gain arbitrary kernel memory read/write on the iOS 10.2/macOS 10.12.

"GHOST TELEPHONIST" IMPERSONATES YOU THROUGH LTE CSFB

Sunday at 11:00 in Track 4
45 minutes | Exploit

Yuwei Zheng, Hacker
Lin Huang, Hacker

One vulnerability in CSFB (Circuit Switched Fallback) in 4G LTE network will be presented. In the CSFB procedure, we found the authentication step is missing. This results in that an attacker can hijack the victim's communication. We named this attack as 'Ghost Telephonist'. Several exploitations can be made based on this vulnerability. When the call or SMS is not encrypted, or weakly encrypted, the attacker can impersonate the victim to receive the "Mobile Terminated" calls and messages or to initiate the "Mobile Originated" calls and messages. Furthermore, Telephonist Attack can obtain the victim's phone number and then use the phone number to make advanced attack, e.g. breaking Internet online accounts. These attacks can randomly choose victims, or target a given victim. We verified these attack with our own phones in operators' network in a small controllable scale. The experiments proved the vulnerability really exists. The attack doesn't need fake base station so the attack cost is low. The victim doesn't sense being attacked since no fake base station and no cell re-selection. Now we are collaborating with operators and terminal manufactures to fix this vulnerability.

SKYTALKS



SCHEDULE POSTED @DCSKYTALKS
+ WWW.SKYTALKS.INFO
+ GRAB A FLYER AT THE ROOM

OFF THE RECORD
NO RECORDINGS ALLOWED
BE THERE OR MISS IT FOREVER

PROMENADE LEVEL, 3RD FLOOR
TURIN/TREVI/VERONA ROOM

WORKSHOPS

WORKSHOP REGISTRATION WAS HELD ONLINE JULY 5TH. THERE IS NO ONSITE REGISTRATION, SIGNUP SHEET, AND ALL SEATS (INCLUDING STANDBY) ARE SOLD OUT. FOR MORE INFO ON THE WORKSHOPS VISIT THE DEF CON WEBSITE. PRE-REGISTRATION WILL BE ONLINE AGAIN FOR DEF CON 26!

THURSDAY

	octavius 1	octavius 4	octavius 5	octavius 6	octavius 7
10:30-14:30	A B C of Hunting Julian Dana	Attacking Active Directory and Advanced Methods of Defense Adam Steed & Andrew Allen	Building Application Security Automation with Python Abhay Bhargav	Introduction to Cryptographic Attacks Matt Cheung	Build Your Stack With Scapy, For Fun and Profit John W. Garrett & João Pena Gil (Jack64)
14:30-18:30	Malware Triage: Malscripts Are The New Exploit Kit Sergei Frankoff & Sean Wilson	Brainwashing Embedded Systems Craig Young, Lane Thames, & Tyler Reguly	Attacking and Defending 802.11ac Networks Vivek Ramachandran	Introduction to Practical Network Signature Development for Open Source IDS Jack Mott & Jason Williams	SDR Crash Course: Hacking Your Way to For Fun and Profit Neel Pandeya, Nate Temple, Wan Liu

FRIDAY

	octavius 1	octavius 4	octavius 5	octavius 6	octavius 7
10:30-14:30	Linux Lockdown: ModSecurity and AppArmor Jay Beale	Scanning the Airwaves: Building a Cheap Trunked Radio/Pager Scanning System Richard Henderson	Introduction to x86 Disassembly Dazzle Cat Duo	Mobile App Attack 2.0 Sneha Rajguru	Applied Physical Attacks on Embedded Systems, Introductory Version Joe FitzPatrick & Syler Clayton
14:30-18:30	Penetration Testing in Hostile Environments: Client & Tester Security Wesley McGrew & Brad Pierce	Windows - The Undiscovered Country Chuck Easttom	Subverting Privacy Exploitation Using HTTP Eijah	Industrial Control System Security 101 and 201 Matthew E. Luallen & Eric Persson	Advanced Wireless Attacks Against Enterprise Networks Gabriel Ryan

SATURDAY

	octavius 1	octavius 4	octavius 5	octavius 6	octavius 7
10:30-14:30	Practical BLE Exploitation for Internet of Things Aditya Gupta	UAC 0day, all day! Ruben Boonen	Edge Cases in Web Hacking John Poulin	Free and Easy DFIR Triage for Everyone: From Collection to Analysis Alan Orlikoski & Dan M	Practical Malware Analysis: Hands-On Sam Bowne
14:30-18:30	Hacking Network Protocols using Kali Thomas Wilhelm & John Spearing	Principals on Leveraging PowerShell for Red Teams Carlos Perez	Windows Post-Exploitation/ Malware Forward Engineering Sean Dillon & Zachary Harding	Pwning Machine Learning Systems Clarence Chio	Harnessing the Power of Docker and Kubernetes to Supercharge Your Hacking Tactics Anshuman Bhartiya

ANDROID TAMER

Saturday from 1000-1150 at Table Three

Anant Shrivastava

Android Tamer is a project to provide various resources for Android mobile application and device security reviews. Be it pentesting, malware analysis, reverse engineering or device assessment. We strive to solve some of the major pain points in setting up the testing environments by providing various ways and means to perform the task in most effortless manner.

Mobile (specifically Android)

<https://androidtamer.com/>

BROPY

Saturday from 1400-1550 at Table Five

Matt Domko

Provides simple anomaly based IDS capabilities using Bro. Bropy parses logs to generate network baselines using a simple Y/N interface, and the accompanying bro script generates logs for traffic outside of the baseline.

<https://github.com/hashtagcyber/bropy>

BULLDOZER

Saturday from 1400-1550 at Table Two

Keith Lee

The tool allows you to supply a username and password that you have captured and cracked from Responder or other sources as well as an IP ranges, subnet or list of IP addresses.

The tool finds its way around the network and attempts to gain access into the hosts, finds and dumps the passwords/hashes, resuses them to compromise other hosts in the network.

Below are some of the places the tools look for hashes/passwords

1. SYSVOL
2. File Shares
3. Memory
4. Tokens (Incognito)
5. MSSQL service credentials
6. Unattend.xml, sysprep.xml, sysprep.inf

It will also exploit the Domain Controller if it's vulnerable to MS14-069 and dump the hashes.

Pillaging the Corporate Network

The tool will also attempt to 'rob' the shares and hosts of the sensitive data/information.

1. Finding files whose filename have the word 'password' in it
2. Dump Wireless. WinVNC, UltraVNC, Putty, SNMP, Windows AutoLogon, Firefox Stored credentials,
3. Find KeePass Databases, FileZilla sitemanger.xml, Apache Httpd.conf, and etc. if they contain credentials.

4. Finding PII data and Credit Card Track Data from memory

5. Browser credentials

It will iterate and continue to test and exploit the systems until all hosts are compromised.

Another useful feature is for attackers who want to find the right credentials in order to access a certain folder under the shares on the host.

For example, \\host1\share\private

You might have the account that allows you to access \\host1\share but you do not know which account you need to access \\host1\share\private.

Using the credentials the tool has captured and finds the 'right key' to the lock.

It is possible to disable any of the options (e.g. no memory search of PAN numbers) so to add a random delay to its operations so as to remain stealth.

We are planning to allow users to develop modules/plugins and encourage development so that its feature set can be extended.

Offense

CELLANALYSIS

Saturday from 1600-1750 at Table Three

Pedro Cabrera

CellAnalysis is one more tool to be added to the pentester arsenal. Nowadays we can find other tools intended to find fake cells, most of them use active monitoring; that is, they monitor traffic coming to the SIM card on a smart phone, so that only cell attacks are scanned on the same network as the SIM card. CellAnalysis offers a different vision, it performs a passive traffic monitoring, so it does not require a SIM card or a mobile device, simply a OsmocomBB phone or compatible device SDR (rillsdr, usrp, hackrf or bladerf) to start monitoring all the frequencies of the GSM spectrum.

Defensive and mobile security

<http://www.fakebts.com/>

HTTPS://CRACK.SH/

Saturday from 1200-1350 at Table Two

David Hulton

Ian FosterCracking DES has been doable for state actors for the past few decades, but most people don't have access to a supercomputer or \$100k of dedicated hardware laying around. In 2012, Moxie Marlinspike and David Hulton released a service for Cloudcracker.com to provide this to the masses for 100% success rate cracking of MSCHAPv2 (PPTP VPNs & WPA-Enterprise). Since then Cloudcracker.com has vanished, but ToorCon has taken over and released <https://crack.sh>, with added features for cracking MSCHAPv1 (Windows Lanman/NTLMv1 login), Kerberos Authentication, and a general purpose interface for cracking other systems that still use DES. We will also be releasing a free real-time service for cracking DES (in ~3 seconds) with chosen-plaintext, providing a full break of Windows Lanman/NTLMv1 authentication and allow people to test their devices to see if they're doing proper WPA-Enterprise certificate checking.

Offense, Mobile, Hardware

<https://crack.sh/>

CRACKMAPEXEC

Saturday from 1400-1550 at Table Three

Marcello Salvati

Ever needed to pentest a network with 10 gazillion hosts with a very limited time frame? Ever wanted to Mimikatz entire subnets? How about shelling entire subnets? How about dumping SAM hashes? Share spidering? Keeping track of all the credentials you pillaged? (The list goes on!) And doing all of this in the stealthiest way possible? Well look no further than CrackMapExec! CrackMapExec (a.k.a CME) is a modular post-exploitation tool written in Python that helps automate assessing the security of "large" Active Directory networks. Built with stealth in mind, CME follows the concept of "Living off the Land": abusing built-in Active Directory features/protocols to achieve it's functionality and allowing it to evade most endpoint protection, IDS and IPS solutions. Although meant to be used primarily for offensive purposes, CME can be used by blue teams as well to assess account privileges, find misconfigurations and simulate attack scenarios. In this demo the author will be showing off v4.0, a major update to the tool bringing more feature and capabilities than ever before! If you are interested in the latest and greatest Active Directory attacks/techniques, weaponizing them at scale and general cool AD stuff this is the demo for you!

Network Defense and Offense

<https://github.com/byt3bl33d3r/CrackMapExec>

CRYPT-KEEPER

Saturday from 1400-1550 at Table Four

Maurice Carey

Crypt-Keeper is a service for securely exchanging files.

Equipment Requirements (Network Needs, Displays, etc): A display or protector would be great. The app will be running on AWS, so a network connection will be needed as well.

Anyone who wants to run a service to securely exchange files.

<https://github.com/mauricecarey/crypt-keeper>

DNS-EXFIL-SUITE

Saturday from 1600-1750 at Table Two

Nolan Berry

Cory SchwartzOur tool kit provides multiple methods of data exfiltration, infiltration and botnet command and control systems using 100% DNS traffic that is either hard to detect or impossible to detect.

I think the best audience here would be PenTesters, DNS Engineers and people looking to learn more about DNS based attack methods.

https://github.com/ndberry/DNS_Exfil_Tool

EAPHAMMER

Saturday from 1600-1750 at Table Five

Gabriel Ryan

EAPHammer is a toolkit for performing targeted evil twin attacks against WPA2-Enterprise networks. It is designed to be used in full scope wireless assessments and red team engagements. As such, focus is placed on providing an easy-to-use interface that can be leveraged to execute powerful wireless attacks with minimal manual configuration. To illustrate how fast this tool is, here's an example of how to setup and execute a credential stealing evil twin attack against a WPA2-TTLS network in just two commands:

```
# generate certificates
```

```
./eaphammer -cert-wizard
```

```
# launch attack
```

```
./eaphammer -i wlan0 -channel 4 -auth ttls -wpa 2 -essid CorpWifi -creds
```

Features:

- * Steal RADIUS credentials from WPA-EAP and WPA2-EAP networks.
- * Perform hostile portal attacks to steal AD creds and perform indirect wireless pivots
- * Perform captive portal attacks
- * Built-in Responder integration
- * Support for Open networks and WPA-EAP/WPA2-EAP
- * No manual configuration necessary for most attacks.
- * No manual configuration necessary for installation and setup process

Offensive security professionals, red teamers, penetration testers, researchers.

<https://github.com/s0lst1c3/eaphammer>

FUZZAPI

Saturday from 1000-1150 at Table One

Abhijeth Dugginapeddi

Lalith Rallabhandi

Srinivas Rao

Fuzzapi is a REST API pen testing tool that automatically does a bunch of checks for vulnerabilities on your APIs. Rather than a tool that only identifies vulnerabilities in web services, we have built a platform that enables everyone to test and understand a large range of API vulnerabilities that exist in both web and mobile applications. After seeing the benefits of Automating REST API pen testing using a basic Fuzzapi tool, the authors have decided to come up with a better version which can automatically look into vulnerabilities in APIs from the time they are written. REST APIs are often one of the main sources of vulnerabilities in most web/mobile applications. Developers quite commonly make mistakes in defining permissions on various cross-platform APIs. This gives a chance for the attackers to abuse these APIs for vulnerabilities. Fuzzapi is a tool written in Ruby on Rails which helps to quickly identify such commonly found vulnerabilities in APIs which

-DEMO LABS-

helps developers to fix them earlier in SDLC life cycle. The first released version of the tool only has limited functionalities however, the authors are currently working on releasing the next version which will completely automate the process which saves a lot of time and resources.

AppSec, Web/Mobile Developers, DevOps

https://www.youtube.com/watch?v=43G_nSTdxLk&t=321s

GIBBERSENSE

Saturday from 1000-1150 at Table Two

Ajit Hatti

On your forensics and investigation assignment found a Gibberish string or unknown file and don't know what it is? Throw it to GibberSense, it might try to make some sense out of it. Not sure if a file is encrypted, encoded or obfuscated using substitution ciphers? GibberSense can give you statistical analysis of the contents and gives you direction for further investigation and also gives you an excellent visualization.

Being an extensible framework, GibberSense gives tools for simple xor encryption, frequency analysis, which gives basic cryptanalysis capabilities. An Open Source Initiative GibberSense is an experimental tool for improving investigations.

Cryptologers, crypt analysts, forensic investigators, developers and testers.

<https://github.com/smxlabs/gibbersense>

GOFETCH

Sunday from 1000-1150 at Table Three

Tal Maor

GoFetch is a tool to automatically exercise an attack plan generated by the BloodHound application.

The tool first loads a path of local admin users and computers generated by BloodHound and convert it to its own attack plan format.

Once the attack plan is ready, it advances towards the destination according to the plan, step by step by successively apply remote code execution techniques and compromising credentials with Invoke-Mimikatz, Mimikatz and Invoke-Psexec.

Enterprise, Applied Security, Windows domain, Defense and offense

A video of the Python version was published here: <https://www.youtube.com/watch?v=dPsLVEORITg>

A video of Invoke-GoFetch will be published soon.

BloodHound Application - <https://github.com/BloodHoundAD/BloodHound>

GREATFET

Saturday from 1200-1350 at Table Three

Dominic Spill

Michael Ossmann

GreatFET is an open source hardware hacking platform. In addition to support for common protocols such as SPI, USB, JTAG, and UART, GreatFET also allows us to implement arbitrary protocols, as well as GPIO and acting as a logic analyser.

Add on boards, known as neighbors, allow us to build on the flexibility of GreatFET and rapidly create new tools. Example neighbors include radio platforms, software defined infrared transceivers, and interfaces for hardware hacking.

Hardware & Offense

Hardware: <https://github.com/greatscottgadgets/greatfet>

Software/firmware: <https://github.com/dominicgs/GreatFET-experimental>

GUMBLER

Sunday from 1200-1350 at Table Two

Willis Vandevanter

The tool searches the entire commit history of a Git project for secrets and files. This is a different approach from other tools which focus on the current revision. It's excellent at digging up API keys, deleted usernames and passwords or files that are now cloaked from .gitignore.

Offense, AppSec

<https://github.com/BufaloWill/gumbler>

HI-JACK-2FACTOR

Sunday from 1000-1150 at Table Six

Weston Hecker

There are several attacks being performed on PKES Passive key entry systems on cars. Several high profile talks this year are about stealing cars using 11 Dollar SDR and cheap devices to relay the signals from the keyfob to the immobilizer. I will be demoing a device that I made using an arduino and a 433/315 Mhz Radio and a 2.4GHZ wireless antenna. They cost about 12 dollars to make and basically add two factor authentication to your vehicle.

Into long explanation

so key fobs in the USA use 315Mhz or 433Mhz which in several of the attack performed this year and in the past people are relaying the input and output of key fobs to start vehicles. My device interrupts all 433mhz and 315 mhz preamble information for a 1 foot radius. and waits for a unscrambled range 2.4 Ghz Bluetooth device to come into range. with a 4 digit pin it will shut down the scrambles blocking the 433/315 respectively. this also works on older RFID enabled keys made in the late 90s early 2000s. I will be demoing the device and all the plans will be released open source MIT licence. in a nutshell it is two factor authentication for most cars for 12 dollars in parts. This will also include a demo of the relay attack being performed on Demo ECU and immobilizer and how the device blocks it.

Offense, Defense, Hardware

<https://eprint.iacr.org/2010/332.pdf>

This was the 2009 research.

Here is the modern 2017 version <https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/>

LAMMA 1.0

Saturday from 1200-1350 at Table One

Antriksh Shah

Ajit Hatti Last year we released LAMMA Beta at DEFCON, this year we are bringing the updated version of LAMMA with new modules for Blockchain Security Testing, auditing Trust stores, enhanced checks for source code analysis and logical flaws in crypto-coding.

LAMMA 1.0 with new features & fixes makes crypto-testing more effective and smoother even for large scale implementations. You can use and enhance LAMMA 1.0, as it's a FREE and OPEN SOURCE.

Cryptologist, crypt analysts, developers and testers, Block Chain and PKI Implements.

<http://www.securitymonx.com/products/lamma>

LEVIATHAN FRAMEWORK

Sunday from 1000-1150 at Table Four

Utku Sen

Özge Barbaros

Leviathan is a mass audit toolkit which has wide range service discovery, brute force, SQL injection detection and running custom exploit capabilities. It consists open source tools such as masscan, ncrack, dss and gives you the flexibility of using them with a combination.

The main goal of this project is auditing as many system as possible in country-wide or in a wide IP range.

Red teamers, penetration testers (Offensive)

Github page: <https://github.com/leviathan-framework/leviathan>

A blog post about it's custom exploit feature:

<https://www.utkusen.com/blog/wide-range-detection-of-doublepulsar-implants-with-leviathan.html>

MALTEGO "HAVE I BEEN PWNED?"

Saturday from 1000-1150 at Table Five

Christian Heinrich

"Have I been pwned?" allows you to search across multiple data breaches to see if your email addresses or aliases has been compromised by LinkedIn, Tumblr, etc

Maltego is a link analysis application of technical infrastructure and/or social media networks from disparate sources of Open Source Intelligence (OSINT). Maltego is listed on the Top 10 Security Tools for Kali Linux by Network World and Top 125 Network Security Tools by the Nmap Project.

The integration of "Have I been pwned?" with Maltego visualises these breaches in an easy to understand graph format that can be enriched with other sources.

Defense

<https://github.com/cmlh/Maltego-haveibeenpwned>

MYCROFT

Saturday from 1400-1550 at Table One

Joshua Montgomery

Mycroft is an open source virtual assistant similar to Siri or Amazon Alexa. The technology stack allows developers to include a voice interface in anything from a Raspberry Pi to a Jaguar FTYPE sports car.

Mycroft integrates Speech-To-Text, Natural Language Processing, a Skill Framework and a Speech To Text engine into a single, easy to deploy software stack.

Though the technology runs anywhere. The company has developed a Raspberry Pi image (Pi-Croft) and recently deployed a Gnome Shell Extension. The company also has a hardware device the "Mark I" that comes pre-loaded with the software and includes a variety of I/O options for directly controlling devices.

Hardware, IoT, Automotive, AI, Everyone

<http://mycroft.ai/>

PCILEECH

Sunday from 1200-1350 at Table Three

Ulf Frisk

Total physical pwnage and plenty of live demos in this action packed Demo Lab! The PCILeech direct memory access attack toolkit was presented at DEF CON 24 and quickly became popular amongst red teamers and governments alike. A year later major operating systems are still vulnerable by default. I will demonstrate how to take total control of Linux, Windows and macOS by PCIe DMA code injection. Kernels will be subverted, full disk encryption defeated, file systems mounted and shells spawned! All this by using affordable hardware and the open source PCILeech toolkit.

<http://github.com/ufrisk/pcileechPIV>

OPACITY

Saturday from 1000-1150 at Table Six

Christopher Williams

OPACITY is a fast, lightweight asymmetric encryption protocol, adopted as an open standard by NIST, ANSI, and Global Platform. OPACITY, originally designed for payment and identity applications, provides a method for securing the NFC channel of low power devices with embedded secure hardware, such as smart cards. I will show an Android demonstration leveraging this open standard, as defined in NIST SP 800-73-4, to securely produce derived credentials and provide flexible and private authentication. While this demo is designed to showcase the Federal PIV standard, the OPACITY algorithm and concepts are broadly applicable to provide secure transactions in IoT, biohacking, and other low power embedded systems.

Authentication, Mobile, Embedded Security, Biohacking

<https://youtu.be/ftn8-Cth554>

-DEMO LABS-

PROBESPY

Sunday from 1000-1150 at Table One

stumblebot

Probespy is a dumb and dirty tool for analyzing directed and broadcast probe request data sent by wifi client devices. It assists in locating where wireless client devices have been (geolocation) and creating behavioral profiles of the person(s) owning the device via the identification of known SSIDs.

offense/recon/surveillance

<https://github.com/stumblebot/probespy>

RADARE2

Saturday from 1400-1550 at Table Six

Maxime Morin

Radare2 is an open-source Reverse-Engineering Framework

A lot of people are currently using radare2 for a large panel of different purposes; binary exploitation, weird CPU architecture reversing, binary diffing, ctf, emulation, We also try to get new contributors for the projects and invite students to collaborate via various platform such as Google Summer Of Code or the Radare Summer of Code we try to organize based on donations.

> Project URL: <http://radare.org/r/>

> Git Project URL: <https://github.com/radare/radare2>

RULER - PIVOTING THROUGH EXCHANGE

Saturday from 1200-1350 at Table Four

Etienne Stalmans

Microsoft Exchange has become the defacto gateway into most organisations. By nature, Exchange needs to be externally accessible, and usually falls outside of normal security monitoring. This can allow for the bypass of common security mechanisms. Even when organisations move into the cloud, their Exchange servers still provide access into the internal environment. It has been shown in the past that abusing the rules feature of Outlook, combined with auto-synchronisation through Exchange, can allow for Remote code-execution.

Furthermore, Exchange offers a covert communication channel outside of the usual HTTP or TCP employed by most malware. Using the mailbox itself, it is possible to create a communication channel that doesn't traverse the normal network boundary, and appears to be normal Exchange behaviour when inspected on the wire.

Introducing Ruler:

During our Red Team assessments, we saw an opportunity to utilise inherent weaknesses of Microsoft Exchange and create a fully-automated tool that aided further breach of the network. Ruler allows for the easier abuse of built in functionality, including the ability to execute code on every mailbox connected to the Exchange server.

This talk will showcase the numerous features of Ruler, demonstrating how to gain a foothold, pop shells on every connected mailbox, use Exchange as a covert communication channel and maintain a near invisible persistence in the organisation. We will also discuss possible defenses against the demonstrated attacks.

<https://github.com/sensepost/ruler>

SAMYKAM

Saturday from 1200-1350 at Table Five

Salvador Mendoza

SamyKam is a new project to pentest mag-stripe information designed using the Samy Kamkar's MagSpoof as base but in this case for Raspberry Pi integration. SamyKam is a portable hardware where the user can interact with it directly on the ssh, OLED, phone or browser to test magnetic card readers or tokenization processes with prepared attacks.

Offense/Defense/Hardware

<https://salmg.net/2017/01/16/samykam/>

SHINOBOT FAMILY

Saturday & Sunday from Saturday 1600-1750, Sunday 1200-1350 at Table Six/Five

ShIn0g1

ShinoBOT Family is a malware suite for the pentester, security engineer who want to test the vendor's solution.

It contains Backdoor, Ransomware, Downloader, Dropper, PowerShell based malware, obfuscation/encryption techniques, Pseudo-DGA, and the C&C is provided as a service (C&CaaS), no fee.

5 sec to get ready and "DOWNLOAD. EXECUTE. CONTROL."

Offense

<https://shinobot.com/> <- ShinoBOT executable

<https://shinobotps1.com/> <- powershell edition

<https://shinolocker.com/> <- ShinoLocker

<https://shinosec.com/> <- other components include ShinoBOT Suite

ADVANCED SPECTRUM MONITORING WITH SHINYSDR

Saturday from 1600-1750 at Table One

Michael Ossmann

Dominic Spill

We have developed open source tools to monitor the RF spectrum at a high level and then drill down to individual signals, supporting both reverse engineering and signals intelligence. By automatically combining the results with OSINT data from regulatory bodies around the world, we are able to build up a picture of devices transmitting in an environment.

Wireless, Defense

<http://greatscottgadgets.com/spectrummonitoring>

SPLUNKING DARK TOOLS - A PENTESTERS GUIDE TO PWNAGE VISUALIZATION

Saturday from 1200-1350 at Table Six

Bryce Kunz @TweekFawkes

Nathan Bates @Brutes_

During a penetration test, we typically collect all sorts of information into flat files (e.g. nmap scans, masscan, recon-ng, hydra, dirb, nikto, etc...) and then manually analyze those outputs to find vectors into target networks. Leveraging data analytics techniques within Splunk, pentesters will be able to quickly find the information they are looking for and hence exploit more target networks within short time periods. This talk covers the required tools for consolidating, analyzing and visualizing the

dark tools that are used by every red team. We'll release the required framework for getting the data where it needs to be, the technical additions to ensure this data is ingested in usable formats, and dashboards for Spunk to leverage this data for mass pwnage of your target!

TRUESEEING: EFFECTIVE DATAFLOW ANALYSIS OVER DALVIK OPCODES

Sunday from 1000-1150 at Table Two

Takahiro Yoshimura (alterakey)

Ken-ya Yoshimura (ad3liae)

Truseeing is an automatic vulnerability scanner for Android apps. It is capable of not only directly conducting data flow analysis over Dalvik bytecode but also automatically fixing the code, i.e. without any decompilers. This capability makes it resilient against basic obfuscations and distinguishes it among similar tools - including the QARK, the scanner/exploitation tool shown by LinkedIn in DEF CON 23. Currently it recognizes most classes of vulnerabilities (as in OWASP Mobile Top 10 (2015).)

AppSec, Mobile

<https://github.com/taky/truseeing>

UNIVERSAL SERIAL ABUSE

Saturday from 1600-1750 at Table Four

Rogan Dawes

Universal Serial aBUse is a combination of hardware and software, and is a refinement of the old school USB HID attacks. It adds a WiFi interface to the USB device, which enables the attacker to remotely trigger the payload at a time of their choosing, not just after a fixed delay from the time it is plugged in. The WiFi interface also enables a back-channel to allow the typed payload to communicate with the attacker without touching the victim's network interfaces.

This enables the attacker to avoid any network complexity (air gaps, firewalls and proxies) or network-based monitoring, and still obtain that precious shell!

This tool is aimed at Offensive folks, with an interest in hardware attacks.

<https://sensepost.com/blog/2016/universal-serial-abuse/>

<https://github.com/SensePost/USaBUse>

VAPOR TRAIL

Sunday from 1200-1350 at Table Six

Galen Alderson

Larry Pesce

AAs red team members and even "evil attackers", we've been finding numerous ways to exfiltrate data from networks with inexpensive hardware: Ethernet, WiFi and cellular (2G, 3G and LTE). The first two are highly detectable, while the latter is expensive and both leave a paper trail. We found a way to use a medium that is right under everypony's nose; low power, broadcast FM radio. With a Raspberry Pi and a length of wire, we can send text and raw binary data with a method nopony (until now) would think to look for. We receive the data with an RTL-SDR, putting our overall hardware budget at \$20.

In this demo, we will show you how to build and use this system. We'll share tales of the custom software and transmission protocols. You want to see it in action? We've got demos. You want the software?

Yep, you can have that too. We're excited to offer Vapor Trail to you, the first FM radio data exfiltration tool. Sure, HAM radio folks have had digital modes for years, but we've done better AND cheaper. We've effectively created our own RF digital mode for pwnage, HAM radio data transfer and redundant communication methods.

Why? Because we can. We want to go undetected with current capabilities. Turns out, our approach is quite novel for pulling data right from a network via pcap or tool output. Offense, Defense, Hardware

<http://vaportrail.io/>

WIDY 2.0: WIFI OWNAGE IN UNDER \$5 RELOADED

Sunday from 1000-1150 at Table Five

Vivek Ramachandran

Nishant Sharma

Ashish Bhangale WiDy is an open source Wi-Fi Attack and Defense platform created to run on the extremely cheap ESP8266 (<\$5) IoT platform. We've written a simple framework which you can hack and create your own tools or automate attack/defense tasks. We also provided code to bring the concept of deception to WiFi area. WiDy was launched in Blackhat Asia 2017 Arsenal and received good response from the audience. WiDy 2.0 release contains several major improvements over initial version.

Attack and Defense

WIFI CACTUS

Saturday & Sunday from Saturday 1000-1150, Sunday 1200-1350 at Table Four

darkmatter

With this project you will be able to listen to all Wi-Fi channels at the same time. No more broken or fragmented frames due to channel hopping. It will passively monitor the dangerous WiFi's around you giving you metadata and actual data that might be useful.

Offense, Defense

<http://palshack.org/>

WIMONITOR - AN OPENWRT PACKAGE FOR REMOTE WIFI SNIFFING

Sunday from 1200-1350 at Table One

Vivek Ramachandran

Nishant Sharma

Ashish Bhangale

WiMonitor is ready to use OpenWRT package which allows the user to convert an OpenWRT WiFi router into a remote WiFi sniffer. It modifies the LuCI interface to show the task-specific configuration option. With the right configuration, it then captures the WiFi packets using monitor mode (while hopping on configured channels) and sends them to the remote machine as Aruba ERM (Encapsulated Remote Mirroring) packets. This allows the user to observe, capture and analyze traffic from multiple sources (read APs turned into sensors) on one machine (laptop/PC) using off the shelf OpenWRT compatible routers.

Defense

-VENDORS-

BREAKPOINT BOOKS



<http://breakpointbooks.com/>

Stop by and browse the wide selection of security-related books on display this weekend. The latest and greatest books available in the industry also include books authored by Def Con presenters. Check out the wide selection of games available

- strategy, card, dice, and deck-building. Buy a game and start playing today.

BUMP MY LOCK



<https://www.bumpmylock.com/>

Bump keys, lock picks and training tools. Bump My Lock has served thousands of customers worldwide since 2007. If we don't have it at the booth, go to our site <http://www.bumpmylock.com>. Free demonstrations and training at our booth.

Bump My Lock is celebrating our 6th year at DEFCON by showcasing our own line of lock picks!! This year, we will feature our Black Diamond sets and our Ruby sets. So come see us for all your Lock Pick Sets, Bump Keys, Clear Practice Locks, Jackknife Pick Sets, Hackware, and more.

Need more help? We have a vast number of articles and videos on lock picking on our blog or your tube channel. If you are a beginner or a master locksmith we have the tools for you.

As always, a percentage of our proceeds will go to the Miracle Match Foundation.

Long live Barcode!

CAPITOL TECHNOLOGY UNIVERSITY



<https://www.capttechu.edu/>

Capitol Technology University, located in Laurel Maryland, offers degrees in engineering, computer science, cybersecurity, and business. Offering online certificates, bachelor's and

master's degrees, which includes a master's in astronautical engineering. As well as doctoral programs in cybersecurity and management and decision sciences. Capitol is regionally accredited by Middle States Association of Colleges.

EFF

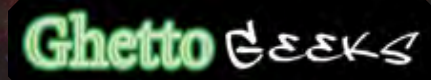


<https://www.eff.org/>

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We defend free speech on the Internet, fight illegal surveillance, support freedom-enhancing technologies, promote the rights of digital innovators, and work to ensure that the rights and freedoms we enjoy are enhanced, rather than eroded, as our use of technology grows. Stop by our table to find out more, pick up some gear, or even support EFF as an official member.

GHETTO GEEKS

Well we're back at it again, and have been working



hard all year to bring you the freshest awesome that we can. If you have been to DEF CON, layerone, toorcon, phreaknic, or other conferences we have been at, you definitely know what so of shenanigans we are up to. If you have never seen us, feel free to come by and take a look at what we have to offer.

Always fun, always contemporary, GhettoGeeks has some for the tech enthusiast (or if you prefer, hacker)

GUNNAR

G U N N A R

<https://gunnar.com/>

GUNNAR Optiks is the only patented computer eyewear recommended by doctors to protect and enhance your vision. Our premium computer eyewear defends eyes from the effects of digital eye strain which can include; dry eyes, headaches, blurry vision, eye fatigue, altered Circadian Rhythms, and insomnia. End the pain of DIGITAL EYE STRAIN.

-PURVEYORS OF FINE HACKER-RELATED MERCHANDISE-

HACKER WAREHOUSE



<http://hackerwarehouse.com/>

HACKER WAREHOUSE is your one stop shop for

hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

HACKERS FOR CHARITY



<http://www.hackersforcharity.org/>

Hackers for Charity is a

non-profit organization that leverages the skills of technologists. We solve technology challenges for various non-profits and provide equipment, job training and computer education to the world's poorest citizens.

HAK5



<https://www.hak5.org/>

Complete your Hacking Arsenal with tools from Hak5 - makers of the infamous WiFi Pineapple, USB Rubber

Ducky, and newly released LAN Turtle. The Hak5 crew, including hosts Darren Kitchen, Shannon Morse and Patrick Norton, are VENDING ALL THE THINGS and celebrating 10 year of Hak5! Come say EHLO and check out our sweet new tactical hacking gear! Everything from WiFi Hot-Spot Honey-Pots to Keystroke Injection tools, Software Defined Radios and Covert LAN Hijackers are available at the Hak5 booth.

HUMAN RIGHTS FOUNDATION



<https://www.hrf.org/>

Human Rights Foundation (HRF) is a nonpartisan nonprofit

organization that promotes and protects human

rights globally, with a focus on closed societies. HRF unites people in the common cause of defending human rights and promoting liberal democracy. Its mission is to ensure that freedom is both preserved and promoted around the world.

KEYPORT®



<https://www.mykeyport.com/>

Keyport® combines keys, pocket tools, &

smart tech into one everyday multi-tool. This year we are bringing our brand new modular product line including the Keyport Slide 3.0 & Keyport Pivot (holds your existing keys), along with our new tech & tool modules which includes a Pocketknife, Bluetooth Locator, and Mini-Flashlight. Sign up for our new Maker Program and design/hack/build your own compatible Keyport modules. Don't forget to bring your keys to the vendor area!

NO STARCH PRESS



<https://www.nostarch.com/>

Thanks to you, we've been publishing books for hackers since 1994. Our titles have personality, our authors are passionate, and our books tackle topics that people care about. We read and edit everything we publish—titles

like Gray Hat C#, Hacking: The Art of Exploitation, Automate the Boring Stuff with Python, Python Crash Course, The Hardware Hacker, and more. This year we're excited to release the PoC || GTFO bible; complete with a leatherette cover, ribbon bookmark, and gilded pages. It's packed with missives from your favorite hackers. Everything in our booth is at least 30% off and all print purchases include DRM-free ebooks. We've got new swag and early access print editions of forthcoming titles like Serious Cryptography, Attacking Network Protocols, and Rootkits and Bootkits.

NUAND



<https://www.nuand.com/>

Nuand develops Software Defined Radio (SDR) platforms for students, hobbyists, and professionals. Their main offering, the bladeRF, is a versatile USB 3.0 device that provides a 300 MHz

-VENDORS-

to 3.8 GHz tuning range, full duplex operation, 12-bit samples at up to 40 MSPS, and an instantaneous bandwidth up to 28 MHz. This device has found a home in application domains including GSM and LTE base stations, digital television, GPS simulation, medical imaging research, and wireless security. Check out their booth to see demos and learn more!

PWNIE EXPRESS



<https://www.pwnieexpress.com/>

Pwnie Express addresses the attack surface exposed by IoT

and connected devices in the enterprise. By continuously discovering, monitoring and assessing all devices on and around a company's network, Pwnie Express provides security professionals the ability to detect, assess and respond to device based threats, including misconfigured, unauthorized, and malicious devices.

The Pwnie Express SaaS platform provides complete device coverage, including IoT, rogue, and traditional IT devices across the entire enterprise. To learn more about Pwnie Express visit www.pwnieexpress.com

RAPID7



<https://www.rapid7.com/>

Rapid7 cybersecurity analytics software and services reduce threat exposure and detect compromise for 4,150 organizations, including 34% of the Fortune 1000. From the endpoint to cloud, we provide comprehensive real-time data collection, advanced correlation, and unique insight into attacker techniques to fix critical vulnerabilities, stop attacks, and advance security programs.

SECURITY SNOBS



<https://securitysnobs.com/>

Security Snobs offers High Security

Mechanical Locks and Physical Security Products including door locks, padlocks, cutaways, security devices, and more. We feature the latest in security items including top brands like Abloy, BiLock, EVVA, KeyPort, Mobeye, Anchor

Las, and Sargent and Greenleaf. Visit <https://SecuritySnobs.com> for our complete range of products. Stop by to see the new and coming soon products in high security and con specials!

SEREPICK



<http://www.serepick.com/>

With the largest selection of lock picks, covert entry and SERE tools available at DEF CON it's guaranteed we will have gear you have not seen before. New tools and classics will be

on display and available for sale in a hands on environment. Our Product range covers Custom Titanium toolsets, Entry Tools, Practice locks, Bypass tools, Urban Escape & Evasion hardware and items that until recently were sales restricted. SPARROWS LOCK PICKS and TOOLS will be displaying a full range of gear including their newly released Core Shims., Sandman and Lock Outs. The WOLF will also be available to the public for the first time in limited quantities. All products will be demonstrated at various times and can be personally tested for use and efficacy.

SHADOWVEX INDUSTRIES



<http://store.shadowvexindustries.com/>

Shadowvex Industries

(SVX) - more than 20 years of pouring blood, sweat & gears into hacker-relevant, limited edition clothing, DJ mixes, stickers, buttons, art prints and more. Miss DJ Jackalope, aka DEFCON's resident DJ mixtress, has been teaming up with us for more than a decade with her own DJ mixes and awesome swag. Follow the music in the vending area to find our booth! If you want to bring home your piece of DEFCON history, you need to get here early - our year-specific designs are only available @DEFCON and only while supplies last!



SIMPLE WIFI



<https://www.simplewifi.com/>

For PenTesting

and unwired Internet Security Specialists: Wireless, WiFi antennas, cables, connectors, USB and Ethernet wireless high power cards and devices, other interesting goodies to be seen only at the table! And new design T-shirts.

-PURVEYORS OF FINE HACKER-RELATED MERCHANDISE-

TOOOL



<http://toool.us/>

The Open Organisation Of Lockpickers is back as always,

offering a wide selection of tasty lock goodies for both the novice and master lockpicker! A variety of commercial picks, handmade picks, custom designs, practice locks, handcuffs, cutaways, and other neat tools will be available for your perusing and enjoyment! Stop by our table for interactive demos of this fine lockpicking gear or just to pick up a T-shirt and show your support for locksport. All sales exclusively benefit TOOOL, a 501(c)3 non-profit organization. You can purchase picks from many fine vendors, but ours is the only table where you know that 100% of your money goes directly back to the hacker community.

UAT



<http://www.uat.edu/>

The University of Advancing Technology (UAT) is a private university located in Tempe, Arizona, offering academic degrees focused on new and emerging technology disciplines. UAT offers a robust suite of regionally

accredited graduate and undergraduate courses ranging from Computer Science and Information Security to Gaming and New Media. UAT has been designated as a Center for Academic Excellence in Information Systems Security Education by the US National Security Agency. Programs are available online and on-campus.

360 UNICORN TEAM



<http://unicorn.360.cn/>

360 Security Research Innovation Alliance consists of many teams, UnicornTeam, RocTeam and PegasusTeam are among them, each team boosts many brilliant

researchers in their corresponding field of focus. UnicornTeam is focusing on wireless security they assess the security of anything that uses radio technologies, from small things like RFID, NFC and WSN to big things like GPS, UAV,

Smart Cars, Telecom and SATCOM. They have presented their researches at premier security conferences like Blackhat, DEFCON, HITB, CanSecWest, RuxCon, POC, SyScan360 etc.

RocTeam is focusing on hardware security research and the R&D of hardwares that can be used for defensive and offensive purposes, they built many hardware security gadgets.

PegasusTeam is focusing on wireless intrusion prevention, wireless threat sensing and wireless penetration test. They have designed and built 'MianYangQiang' to demonstrate the threats of public WIFI, wireless honeypot, wireless intrusion prevention system '360TianXun' which have been widely deployed city wide and in enterprises.

UNIX SURPLUS



<https://unixsurplus.com/>

"Home of the \$99 1U Server"

1260 La Avenida St Mountain View, CA 94043
Toll Free: 877-UNIX-123 (877-864-9123)

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>.

HACKERBOXES



www.hackerboxes.com

HackerBoxes is the subscription box service for DIY electronics and hardware hacking. Each monthly HackerBox includes a carefully curated collection

of projects, components, modules, tools, supplies, and exclusive items. HackerBox Hackers are electronics hobbyists, makers, hardware hackers, and computer enthusiasts. Many connect through social media channels to create a community of experience, support, and ideas. Let's see what you make with your HackerBoxes.

BOOK SIGNINGS!

Where: No Starch Press, in the vendor area, on promenade level.

FRIDAY:

12:00 - David Thiel, iOS Application Security

13:00 - PoC | | GTFO Group Signing

14:00 - James Forshaw, Attacking Network Protocols

14:30 - Al Sweigart, Automate the Boring Stuff with Python

15:00 - Jon Erickson, Hacking: The Art of Exploitation, 2nd Edition

SATURDAY:

11:30 - Cory Doctorow, Walkaway

13:00 - Craig Smith, The Car Hacker's Handbook

14:00 - Eugene Rodionov & Alex Matrosov, Rootkits and Bootkits

15:00 - Nick Cano, Game Hacking

15:30 - Violet Blue, The Smart Girl's Guide to Privacy

CONTEST CLOSING CEREMONIES

WANNA KNOW WHO IS THE BEST AT FINDING RANDOM STUFF AROUND LAS VEGAS DURING DEF CON? CURIOUS WHO IS THE BEST AT SOCIAL ENGINEERING SOMEONE INTO GIVING UP PRIVILEGED PERSONAL OR COMPANY DATA? WHAT ABOUT THE BEST TEAM TO BE HARASSED, FED LOTS OF BOOZE AND STILL ABLE TO WRITE AND COMPILE EPIC CODE?

COME JOIN US AS WE ANNOUNCE THE WINNERS OF THE DEF CON 25 CONTESTS AT OUR CONTESTS CLOSING CEREMONIES, FROM 14:00 - 15:30PM ON THE STAGE ON THE MAIN CONTEST FLOOR!

BLACK BADGE WINNERS WILL BE ANNOUNCED DURING THE MAIN CLOSING CEREMONIES AT 16:30PM IN TRACKS 3 & 4

-THURSDAY-

	101 Track 1	101 Track 2
10:00	There's no place like 127.0.0.1 - Achieving reliable DNS rebinding in modern browsers Luke Young	Where are the SDN Security Talks? Jon Medina
11:00	From Box to Backdoor: Using Old School Tools and Techniques to Discover Backdoors in Modern Devices Patrick DeSantis	Opt Out or Deauth Trying !- Anti-Tracking Bots Radios and Keystroke Injection Weston Hecker
12:00	Porosity: A Decompiler For Blockchain-Based Smart Contracts Bytecode Matt Suiche	Jailbreaking Apple Watch Max Bazaliy
13:00	Amateur Digital Archeology Matt 'openfly' Joyce	Wiping Out CSRF Joe Rozner
14:00	Hacking the Cloud Gerald Steere & Sean Metcalf	See No Evil, Hear No Evil: Hacking Invisibly and Silently With Light and Sound Matt Wixe
15:00	Inside the "Meet Desai" Attack: Defending Distributed Targets from Distributed Attacks	Real-time RFID Cloning in the Field Dennis Maldonado
15:20	CINCVoFLT (Trey Forgety)	Exploiting Old Mag-stripe information with New technology Salvador Mendoza
16:00	DEF CON 101 Panel HighWiz, Malware Unicorn, Niki7a, Roamer, Wiseacre, & Shaggy	The Last CTF Talk You'll Ever Need: AMA with 20 years of DEF CON Capture-the-Flag organizers Vulc@n, Hawaii John, Chris Eagle, Invisigoth, Caesar, & Myles
17:00		

-FRIDAY-

	DEF CON 101	Track 2	Track 3	Track 4
10:00	macOS/iOS Kernel Debugging and Heap Feng Shui Min(Spark) Zheng & Xiangyu Liu	Welcome to DEF CON 25 The Dark Tangent		Secret Tools: Learning About Government Surveillance Software You Can't Ever See Peyton "Foofus" Engel
10:20	Offensive Malware Analysis: Dissecting OSX/FruitFly via a Custom C&C Server Patrick Wardle	Hacking travel routers like it's 1999 Mikhail Sosonkin	The Brain's Last Stand Garry Kasparov	Panel: Meet The Feds
11:00	Rage Against the Weaponized AI Propaganda Machine Suggy (AKA Chris Sumner)	Weaponizing the BBC Micro:Bit Damien "virtualabs" Cauquil	Hacking Smart Contracts Konstantinos Karagiannis	Andrea Matwyshyn, Terrell McSweeney, Dr. Suzanne Schwartz, & Leonard Bailey
12:00	CITL and the Digital Standard - A Year Later Sarah Zatzko	Open Source Safe Cracking Robots - Combinations Under 1 Hour! (Is it bait? Damn straight it is.) Nathan Seidle	A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages! Orange Tsai	Hacking Democracy: A Socratic Dialogue Mr. Sean Kanuck
13:00	Controlling IoT Devices With Crafted Radio Signals Caleb Madrigal	Teaching Old Shellcode New Tricks Josh Pitts	Starting the Avalanche: Application DoS In Microservice Architectures Scott Behrens & Jeremy Heffner	Next-Generation Tor Onion Services Roger Dingledine
14:00	Using GPS Spoofing to Control Time David "Karit" Robinson	Death By 1000 Installers; on MacOS, It's All Broken! Patrick Wardle	Breaking the x86 Instruction Set Christopher Domas	How We Created the First SHA-1 Collision and What it means For Hash Security Elie Bursztein
15:00	Assembly Language is Too High Level XlogicX	Phone System Testing and Other Fun Tricks "Snide" Owen	Dark Data Svea Eckert & Andreas Dewes	Abusing Certificate Transparency Logs Hanno Böck
16:00	Radio Exploitation 101: Characterizing, Contextualizing, and Applying Wireless Attack Methods Matt Knight & Marc Newlin	The Adventures of AV and the Leaky Sandbox Itzik Kotler & Amit Klein	An ACE Up the Sleeve: Designing Active Directory DACL Backdoors Andy Robbin & Will Schroeder	"Tick, Tick, Tick. Boom! You're Dead." - Tech & the FTC Whitney Merrill & Terrell McSweeney
17:00	Cisco Catalyst Exploitation Artem Kondratenko	Panel - DEF CON Groups	MEATPISTOL, A Modular Malware Implant Framework FuzzyNop (Josh Schwartz) & ceyx (John Cramb)	The Internet Already Knows I'm Pregnant Cooper Quintin & Kashmir Hill

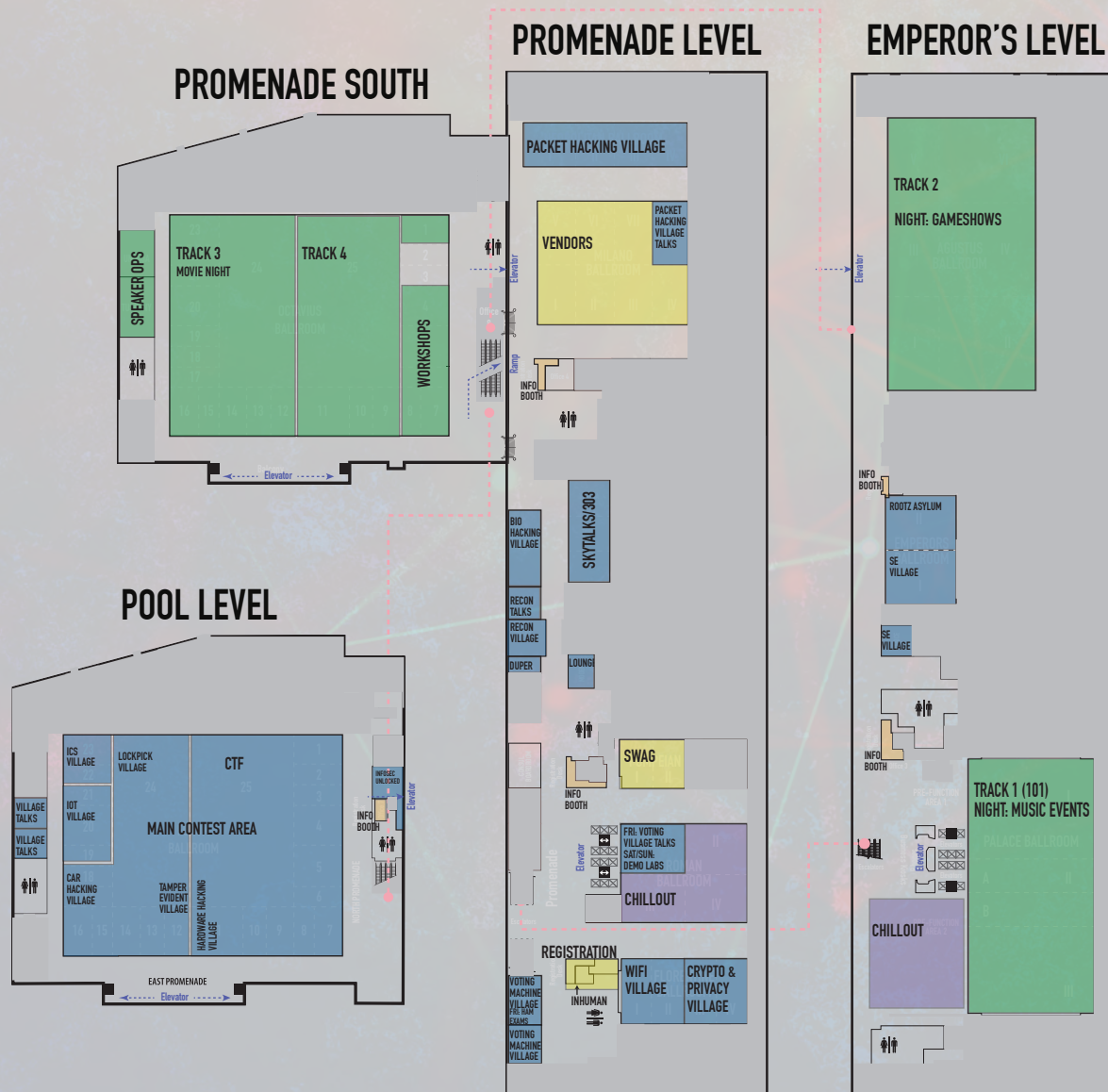
-SATURDAY-

	DEF CON 101	Track 2	Track 3	Track 4
10:00	Persisting with Microsoft Office: Abusing Extensibility Options William Knowles	\$BIGNUM Steps Forward, \$TRUMPNUM Steps Back: How Can We Tell If We're Winning? Cory Doctorow	Get-\$pwnd: Attacking Battle-Hardened Windows Server Lee Holmes	The spear to break the security wall of S7CommPlus Cheng
10:20	Breaking Wind: Adventures in Hacking Wind Farm Control Networks Jason Staggs		WSUSpendu: How to Hang WSUS Clients Romain Coltel & Yves Le Provost	(Un)Fucking Forensics: Active/Passive (i.e. Offensive/Defensive) Memory Hacking/Debugging. K2
11:00	Microservices and FaaS for Offensive Security Ryan Baxendale	Secure Tokin' and Doobiekeys: How to Roll Your Own Counterfeit Hardware Security Devices Joe FitzPatrick & Michael Leibowitz	If You Give a Mouse a Microchip... It Will Execute a Payload and Cheat At Your High-stakes Video Game Tournament skud (Mark Williams) & Sky (Rob Stanley)	Evading Next-Gen AV Using Artificial Intelligence Hyrum Anderson
11:20	Abusing Webhooks for Command and Control Dimitry Snezhkov			All Your Things Are Belong To Us
12:00	Driving down the rabbit hole Mickey Shkatov, Jesse Michael, & Oleksandr Bazhaniuk	When Privacy Goes Poof! Why It's Gone and Never Coming Back Richard Thieme a.k.a. neuralcowboy	DNS - Devious Name Services - Destroying Privacy & Anonymity Without Your Consent Jim Nitterauer	Zenofex, 0x00string, CJ_000, & Maximus64
13:00	Demystifying Windows Kernel Exploitation by Abusing GDI Objects. 5A1F (Saif El-Sherei)	Koadic C3 - Windows COM Command & Control Framework Sean Dillon (zerosum0x0) & Zach Harding (Aleph-Naught-)	Twenty Years of MMORPG Hacking: Better Graphics, Same Exploits Manfred (@_EBFE)	A Picture is Worth a Thousand Words, Literally: Deep Neural Networks for Social Stego Philip Tully & Michael T. Raggo
14:00	Attacking Autonomic Networks Omar Eissa	Trojan-tolerant Hardware & Supply Chain Security in Practice Vasilios Mavroudis & Dan Cvrcek	Linux-Stack Based V2X Framework: All You Need to Hack Connected Vehicles p3n3troot0r (Duncan Woodbury) & ginsback (Nicholas Haltmeyer)	XenoScan: Scanning Memory Like a Boss Nick Cano
15:00	MS Just Gave the Blue Team Tactical Nukes (And How Red Teams Need To Adapt) Chris Thompson	Tracking Spies in the Skies Jason Hernandez, Sam Richards, & Jerod MacDonald-Evov	D00Med Point of Sale Systems trixr4skids	Digital Vengeance: Exploiting the Most Notorious C&C Toolkits Professor Plum
16:00	Dealing the Perfect Hand - Shuffling Memory Blocks On z/OS Ayoul3	From "One Country - One Floppy" to "Startup Nation" - The Story of the Early Days of the Israeli Hacking Community, and the Journey Towards Today's Vibrant Startup Scene Inbar Raz & Eden Shochat	CableTap: Wirelessly Tapping Your Home Network Marc Newlin, Logan Lamb, & Chris Grayson	Game of Drones: Putting the Emerging "Drone Defense" Market to the Test Francis Brown & David Latimer
17:00	Here to stay: Gaining persistency by Abusing Advanced Authentication Mechanisms Marina Simakov & Igal Gofman	Taking Windows 10 Kernel Exploitation to the next level - Leveraging write-what-where vulnerabilities in Creators Update Morten Schenk	Introducing HUNT: Data Driven Web Hacking & Manual Testing Jason Haddix	Popping a Smart Gun Plore

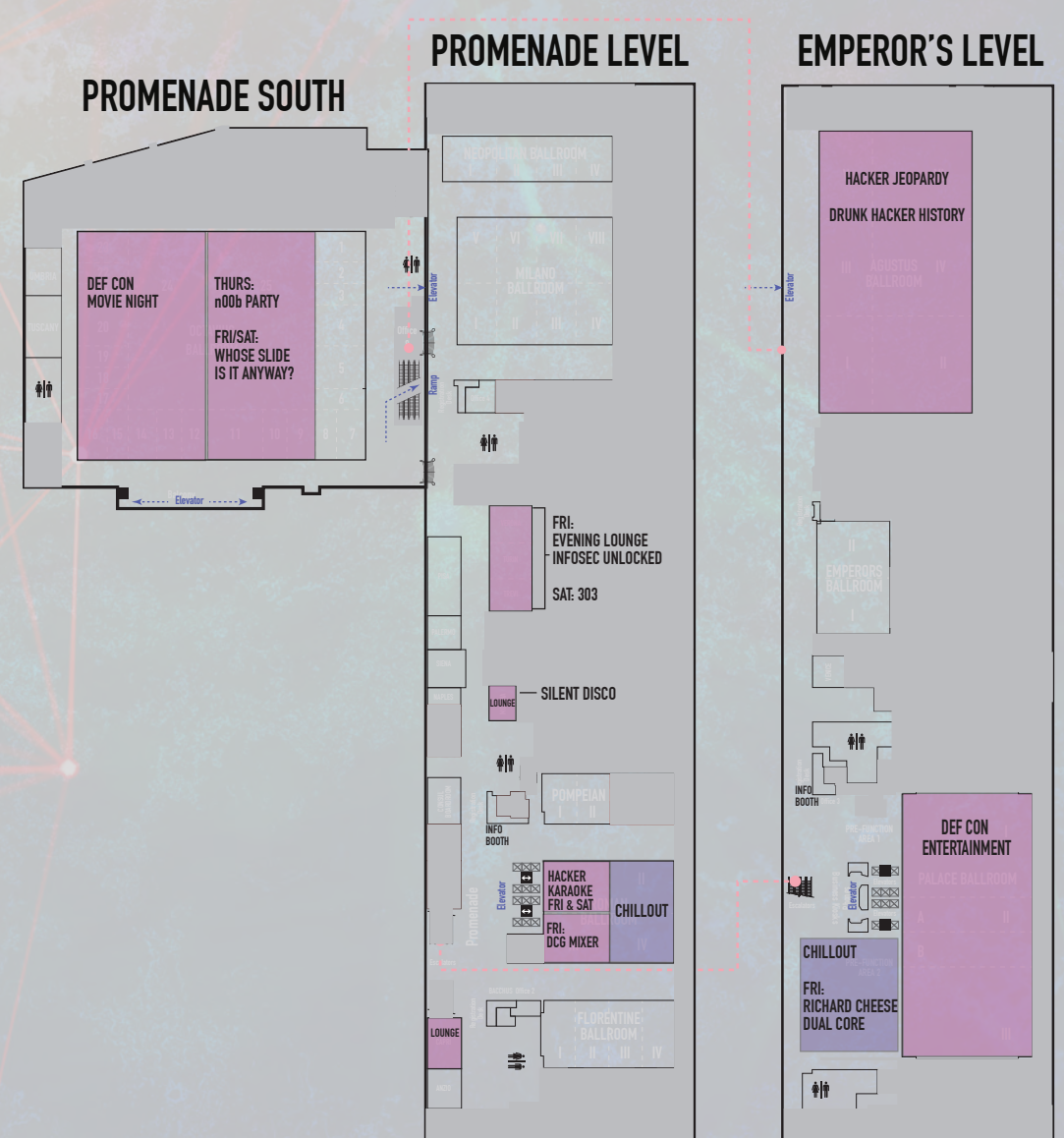
-SUNDAY-

	DEF CON 101	Track 2	Track 3	Track 4
10:00		I Know What You Are by the Smell of Your Wifi Denton Gentry	Breaking Bitcoin Hardware Wallets Josh Datko & Chris Quartier	Untrustworthy Hardware and How to Fix It Octane
10:20	Unboxing Android: Everything You Wanted To Know About Android Packers Avi Bashan & Slava Makkaveev	PEIMA (Probability Engine to Identify Malicious Activity): Using Power Laws to address Denial of Service Attacks Redezem	BITSInject Dor Azouri	Ghost in the Droid: Possessing Android Applications with ParaSpectre chaosdata
11:00	Total Recall: Implanting Passwords in Cognitive Memory Tess Schrodinger	Backdooring the Lottery and Other Security Tales in Gaming over the Past 25 Years Gus Fritschie & Evan Teitelman	Exploiting Continuous Integration (CI) and Automated Build systems spaceB0x	Ghost Telephonist' Impersonates You Through LTE CSFB Yuwei Zheng & Lin Huang
12:00	The Black Art of Wireless Post Exploitation Gabriel "solstice" Ryan	Are all BSDs are created equally? A survey of BSD kernel vulnerabilities. Ilja van Sprundel	The Call Is Coming From Inside the House! Are You Ready for the Next Evolution in DDoS Attacks? Steinthor Bjarnason & Jason Jones	Genetic Diseases to Guide Digital Hacks of the Human Genome: How the Cancer Moonshot Program will Enable Almost Anyone to Crash the Operating System that Runs You or to End Civilization... John Sotos
13:00	Game of Chromes: Owning the Web with Zombie Chrome Extensions Tomer Cohen	Bypassing Android Password Manager Apps Without Root Stephan Huber & Siegfried Rasthofer	Malicious CDNs: Identifying Zbot Domains en Masse via SSL Certificates and Bipartite Graphs Thomas Mathew & Dhia Mahjoub	Revoke-Obfuscation: PowerShell Obfuscation Detection (And Evasion) Using Science Daniel Bohannon (DBO) & Lee Holmes
14:00	Call the Plumber - You Have a Leak in Your (Named) Pipe Gil Cohen	Weaponizing Machine Learning: Humanity Was Overrated Anyway Dan "AltF4" Petro & Ben Morris	Man in the NFC Haoqi Shan & Jian Yuan	Friday the 13th: JSON attacks! Alvaro Muñoz & Oleksandr Mirosh
15:00		25 Years of Program Analysis Zardus (Yan Shoshitaishvili)		
16:30			Closing Ceremonies	
17:00				

DEF CON 25 Floorplan CAESAR'S PALACE CONFERENCE CENTER



DEF CON 25 Floorplan - Nocturnal CAESAR'S PALACE CONFERENCE CENTER



-SHOUT OUTS-

I'd like to thank everyone who supports DEF CON, either by running a contest, workshop, speaking, playing music, planning a event, throwing a party, being a hacker community vendor, or just engaging with the community.

I also want to specifically thank all the people and departments of DEF CON who put their time in year round to make this con possible. As you can see by the lists below there are hundreds of them, and I am amazed and humbled by their work each year.

A special thank you to Aruba Networks who donated 75 AP-305s for DC25, on top of the APs and controllers they donated a couple of years ago. Thanks to them we can retire the AP-70s and AP-65s that were purchased back in 2005/2006 that have served us well for over a decade.

Finally I'd also like to thank the Caesar's hotel teams, the CTF competitors, speakers, and events organizers, and all the others behind the scenes. A special thank you to the back end staff of Charel, Jeff, Nikita, Neil, Darington, Mar, Janet, and Will, who all help the trains run on time. THANK YOU!

- The Dark Tangent

Arts & Entertainment: ChrisAM would like to thank everyone responsible for this year's entertainment & decor: Krisz Klink, Great Scott, Zziks, Mindy, djdead, CTRL, Zebbler Studios, Mobius, and SomaFM.

Contests, Events, Villages: Grifter would like to thank every Goon on the Contests, Events, Villages, Parties, and Demo Labs team. Many thanks to 0x58, Apexxor, ArmyTra1n3d, BoKnows, Br00zer, Config, Cube, Drizzt, heisenberg, jinteki, m0hgarr, Mack, phartacus, phorkus, Respondo, Saltr, Secove, Sketch, Stumper, Xploit, Zant, and Ziggy for the long hours and late nights; this wouldn't be possible without you guys. A HUGE thank you goes to the DEF CON HQ team, Nikita, Neil, Darington, Charel, Will, and of course, The Dark Tangent, for dealing with one of the most insane planning years I've seen in my 17 years as a Goon. (They also get my apologies for the stress I constantly add to them, I love you guys.)

Lastly, to the many organizers that have filled DEF CON with countless contests, villages, events, parties, and just plain mayhem, for the past 25 years...Thank You! Keeping 20,000+ hackers entertained in new and challenging ways may actually be the biggest challenge of them all, and you make it look easy.

Content: Nikita would like to thank the DEF CON 25 Reviewers for their help in selecting the content for DEF CON. Through countless hours, sleepless nights, tense gif wars, and heavy deliberation we came together to provide hackers with: 4 speaking tracks, 4 days of content, 3 days of workshops, and several evening lounges. Thank you tremendously to all the speakers, co-speakers, and workshop instructors who've brought their content to us and made it accessible to the very hacker community we all love so much.

CFP Board: The Dark Tangent, Leah, Jericho, High Wizard, Shaggy, Roamer, Claviger, Zoz, Medic, Suggy, PWCrack, ZFasel, Malware Unicorn, CrYpT, SecBarbie, Yan, Dead Addict, Wiseacre, Weasel, Vulc@n, Singe, Vyrus, Grifter. Special Reviewers: Wonk, Mouse, snow, Andrea Matwyshyn, Tuna. Workshop Reviewers: Ash, Da Kahuna, Highwiz, Leah, Munin, CyberSulu, Beaker, Tottenkoph.

DC Forums: TheCotMan gives thanks to all the volunteers that help keep the forums running. Shout-out thanks to present admins: Dark Tangent and Neil. Shout-out thanks to present mods: AlxRogan, blakdayz, noid, astcell, and Thorn. Double thanks to Dark Tangent for buying hardware, getting us Internet access, and required software to run the forums, and for working on the system when things fail. Thanks to Grifter and the CVE department for Contests/Villages/Events information synchronization with matching CVE forums.

Thanks to DCG department for notices on forums for new/expired DCG. Thanks to goons for gooning. This is my 13th year as an Admin (and a moderator even longer) and in all these years, I've failed to thank the users: Thanks to the users that pose questions, and users that answer them. Thanks to users that provide feedback after DEF CON on how to make it better and users that pose complaints and suggestions to resolve them. Thank you users!

Dispatch: RF and Ahab would like to thank the Dispatch staff: AsmodianX, Voltage Spike, Mat, BonBon, Fosgood, Tony, KODEZ, LOG1C, Craig, w00k, dll3ma, Maj, and Ben.

InfoBooth: Mello and LittleBruzer would like to thank all the InfoBooth goons for bad information and sending humans in the wrong direction:

OxNBE1, Artifakt, Banasidhe, Big, Doug, Boudica, Cheshire, Chris, Drew, Jerel, Jixion, Khadija, Littleroo, MajorMayhem, Medic, PEZHead, Sanchez, ScurryFool, Seth, Sl33pE, TACSAT, Telecon, algorithn, dara, deety, jimi2x, krav, madstringer, n00bz, p0lr, telecommunist, titot

Inhuman Reg: Inhuman reg would like to thank: Nikita, Neil, Cstone, Sauce, Drizzt, Charel, Will, Shaggy, Mouse, Anne, Pyr0, Agent X, Hony, Maggie, and everyone who stepped forward to help create & prepare the badges for 25,000 hackers. By the time DEF CON starts we've put in months of planning, organizing, and coordination. We're proud of the small dedicated team that's spent a week on site before con, assembling thousands of Human & Inhuman Badge registration bags so that LineCon has an expedient and joyous d nouement.

NOC: Wow, DEF CON 25! As usual effffn and DEF CON would like to thank all the efforts of our industrious NOC team, they put a lot of work in so you guys can enjoy the con.

By the time you're reading this, months of planning happened and crazy few implementation days on site have been lived to cover everything we do for the con. From requests to

attend all of the vendors, speakers, press, contests, attendees to those awesome DC TV channels for your enjoyment along with your hangover in the your hotel room.

mac, videoman, #sparky, booger, CRV, naifx, c0mmiebstnd, serif, c7five, Jon2, James and Mansi dedicated a great portion of their DEF CON 25 expedition to making sure everything breaks (and if it does, to fix it right away). If you run into any of them, please make sure you buy them a beverage, will ya?

The entire NOC team would like to thank the Caesar's IT and Encore for the tireless support in making it all happen.

Lastly, looking back to 25 years of DEF CON, I would like to also thank all of those who did good things for the NOC along the way, especially: Lockheed, Heather, Derek, Sqweak, t34se, rukbat and arh@wk.

Photo: DEF CON Photo Goons would like to thank: Viss, ASTCell, Cannibal, Loather and InfoSystir.

Press: A Big Thank You to all the press who not only cover the DEF CON community, but are part of it, as well as all the Press Goons who support the press who are covering DEF CON: Melanie, Sylvia, Tracy, Jeff, Alan, David, Lin, Linda, Heather, Monika, Alex.

Production: Charel in Production would like to thank: C0njur3r, kampf, Ouze1, Betsy, Ira, Killerspud, Spencural, jup1t3r, Chunk, supertechguy, L34N, metacortex, A, and skyria. Call us when you need us!

QM: QM Stores would like to thank Caesar for coming up with his famous "Veni Vidi laceratus" quote, and also for conquering those pesky Goths. We recognise Marc Antony for being a player and Cleopatra for being a saucy minx. ETA, Sunsh1ne, Zac, Waz, Buttersnatcher, MultiGrain, Saint, Youngblood, Lord Drimacus, Geo, Shell_E, Seven, Red Ace, Mr. Bot, Noise, Big Easy, Cell Wizard and Agent X for just being plain awesome and all the Goons for being Goons on a hot hot weekend in Vegas. Feds for being sneaky and conspicuous and Black Hats for keeping it real. White Hats, Red Teams, Blue Teams and their pimps for keeping the wolf from the door. We're also quite grateful for all the Humans who give a small spark of meaning to our otherwise pointless and desolate little lives, and give us a reason to get up at "Oh Dark Early" and work until "Is That The Fucking Time?" in order to dispense shiny. We love our DEF CON family! See you next year! Major Malfunction.

Registration:Reg shout outs: TW; Tyler and Matt; SOC, QM, Swag, and Info Booth; the line wranglers; anyone anywhere who spends their con moving heavy stuff from one place to another; and the attendees, as always, for their patience.

SOC: Cjunky and tacitus would like to thank AdaZebra, AK81, Alex C, Amber, Angie, arcon, Ast0r, Atriyann, atropine, b3l, BeaMeR, Blakdayz, Br1ck, Carric, Chosen1, CHRIS, Crusader, cymike, Dallas, Darkwolf, deelo, dr.kaos, DrFed, Duckie, echosixx, Faz, FoxCaptain, fr0gg3r, gadams, George, Glasswalk3r, GodFix, Hamster, Hattori

Hanzo, iole, JAFO, John Doll, Judo, k3rn3l, Kallahar, KRS, kruger, Lordy, M0rph1x, mattrix, mauvehed, MAXIMUS, MIM, n1cFury, n3x7, NextInLine, Nohackme, Nothingness, P33v3, ph3r, Phat Hobbit, Plasma, polish_dave, Precore, Priest, Rabbit, RadioActive, Raven, Red, SAGE, Shib, Siviak, sl3dge, Slick, SomeNinja, Sonicos, sp00ns, Spedione, stan, stealth, Sumdunce, Synn, TBD, TieFighter, timball, WarFlower, Wetod, wham, Wheels, WhiteB0rd, wilnix, winx, Wreaktifier, xenophyx, xtremelatino, and zerofux.

We also wish to honor Goons who have retired, some after 10+ years of Gooning: Arclight, captain, chs, crzyhrse, cyber, Danozano, dc0de, flea, freshman, Gadsden, godminusone, Gonzo, Jake, JustaBill, Krassi, Londo, lunaslide, noid, Nynex, Pappy, Pescador, Queeg, quiet, rik, riverside, SkyDog, Vidiot.

Finally, a very special thanks goes out to all SOC Goons who have given their time, treasure, blood, sweat and tears over the past 25 years. Pax Per Imperium.

Speaker Ops: Proctor would like to thank the Speaker Operations staff for another year of great service to DEF CON and its speakers. These goons are pwcraack, Mnky, idontdrivecars, Shadow, Goekesmi, Crash, Jur1st, Scout, Bitmonk, Bushy, notkevin, Pasties, CLI, Jinx, gattaca, roundRiver, Vaedron, K-hole, St0neHouse, Jutral, Surreal_Killer, Milhouse, Flattire, phliKtid, Snarf, C@spcr, daKahuna, mubix, #s0sayw3all, Cursor, shortcake and AMFYOYO!

Swag: Secret would like to thank all the Swag Goons: lisa133, Dasha, gingerjet, spiggy, Serenity, furysama, Pelican, Themikeconnor, gLoBuS, Bearclaw, Mr.Katt, 5kyf4ll, Magnar, daedala, 10rn4, Brizan, redacted, Heal, and Chade for all their hard work, and all the other departments for what they do to make a great con!

Vendors: HexdumP and PushPin from vendors would like to take a moment to recognize everyone who has participated in DEF CON over the past twenty five years. The environment, culture, and the community that we know today has been built by working together with Production, Network and Dispatch, QM, the Safety Goons, our vendors, and even our attendees.

Year after year it becomes more apparent how everyone, regardless of department, is willing to step up and help one another out. Wiseacre, CrYpT, Wad, AlxRogan, Jenn, latenite, redbear, and Pinball have done a fantastic job in making sure that DC25 goes as smoothly as possible for both our vendors and attendees. Lastly, the vendor area just wouldn't have been the same if anyone other than Roamer, he has set the standard that we all are working towards achieving each year. Thank you again to everyone.

Workshops: Tottenkoph thanks all of those who worked to review the workshop proposals this year, Neil and Nikita for all of the hard work and help they do, and her amazing team of goons for the effort they're putting in. Thank you: Beaker, CyberSulu, Joel, Jen, SinderzNAshe, Jay, Flipper, Fallible, Brian, RandomInterrupt, BinaryBuddha. She would also like to give a shout-out to the QM, production, and SOC departments for their support.

