
HACK WITH US

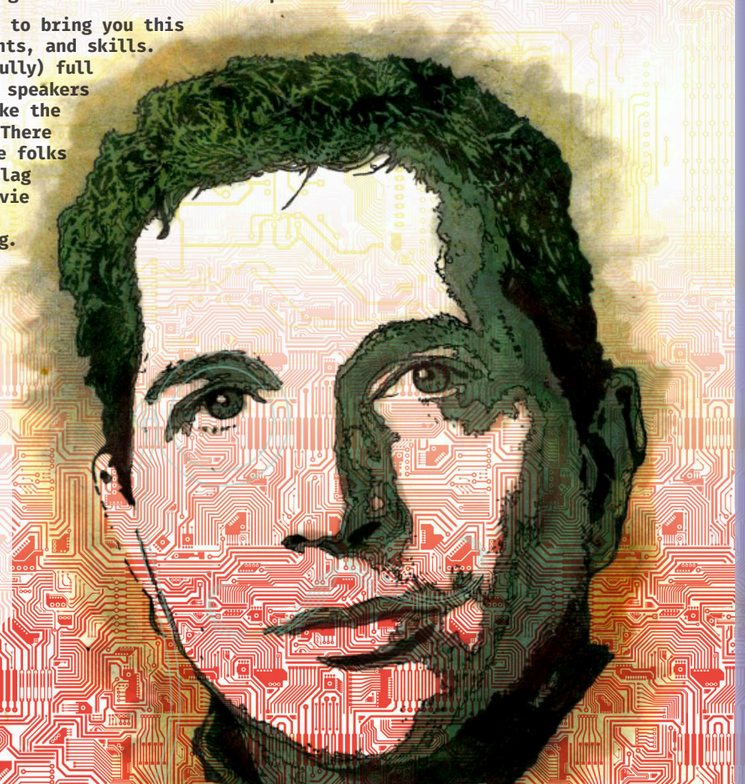
Welcome to DEF CON 22!

This year we are working with a loose theme of “behind the curtain”, an idea Nikita came up with after re-watching the classic movie “They Live”. It fits well with the hacker world, where nothing is as simple as it first seems, and there is always one more step, one more thing to learn, some secret to learn and some forbidden knowledge to hold on it. Now take that to the next level with all the leaks, revelations about hardware backdoors, intercepts, companies purposefully adding surveillance features, and sys admins being targeted and you can go full paranoid! It's ok! Let it all out. Deep breath.

Last year I spoke about how offense has overwhelmed defense, and how it led to a sense of helplessness. Its been a year and has sunken in for all of us. No more false illusions. Currently offensive is in the middle of a “presumptive close” attack. If we accept defense is futile because offense always wins, then we all stop trying as hard. We focus on cleanup instead of prevention. For me the path forward is clear. Radical simplicity around what you must trust. Accept less features for more reliability. Demand less to get more. Why use a switch when a crossover cable will do?

The security, hacker, and engineering world has responded to this reality with code audits, a push for DNSSEC, DANE, pervasive encryption, and renewed interest in privacy technology. The policy folks have focused on transparency reports, disclosure rules, and started a debate about the role of governments purchasing 0day exploits. There is a vibrancy I haven’t seen in years, a sense that we can all make a difference, that our skills can help the public, and we are being looked to as an alternative to big brother. Don’t fuck it up!

Over 300 volunteers have worked behind the scenes to bring you this event, constantly reinventing their contests, events, and skills. This year we have an electronic badge with (hopefully) full secret release of its dev kit, a great line up of speakers and expanded villages with many new additions, like the privacy village, SE village, and a SCADA village! There is also a Packet Hacking Village, organized by the folks that brought you the Wall of Sheep. Capture The Flag has reorganized to be more spectator friendly. Movie night is screening two new films with either the directors or actors. The core network is now 10gig. The internet connection is at maximum. Heck even the font size for this program has gone from 6.8 to 8.1!



We strive to make a large conference like DEF CON feel small, to give everyone a chance to meet new people and make new friends. From more villages, longer chill out hours, a larger space for the DEF CON Forum meetup, to the Dusk ‘till Con event spaces we strive to create a balance of tech and social. We can only do so much, and like most things in life it all comes down to you. We’ve built the environment, now the con is what you make of it!

The Dark Tangent

contents

the network

DefCon-Open : Type: Open / 2.4 and 5 Ghz
DefCon : Type: WPA2/ 802.1x

Just like the past few years the DEF CON NOC works hard to provide you the internetz via WiFi access throughout the Rio convention center. There are two official ESSIDs: the encrypted and cert/user-based authentication (DefCon) and the unencrypted free-for-all one (DefCon-Open): choose wisely. Most of the devices these days should be 802.1x compatible, so not only configure it properly to enjoy the GHz but also remember you’re at a hacker conference. Create your credentials and download the digital certificate at https://wifireg.defcon.org but please take your time to pick a password that is not used anywhere else, like your work Windows domain.

Also, keep an eye out on http://www.defconnetworking.org for stats, data and most important updates about the network during and post-con.

And, believe it or not, we want your feedback: noc@defconnetworking.org

DEF CON TV

Once again, you can nurse your hangover watching the talks in your hotel room. DC TV brings the DEF CON talks to you. Turn on the TV, grab your favorite beverage and don’t forget to shower.

Track 1: Ch55, Track 2: Ch56, Track 3: Ch57

P&T Theater: Ch58, Info / DEF CON Radio: Ch59

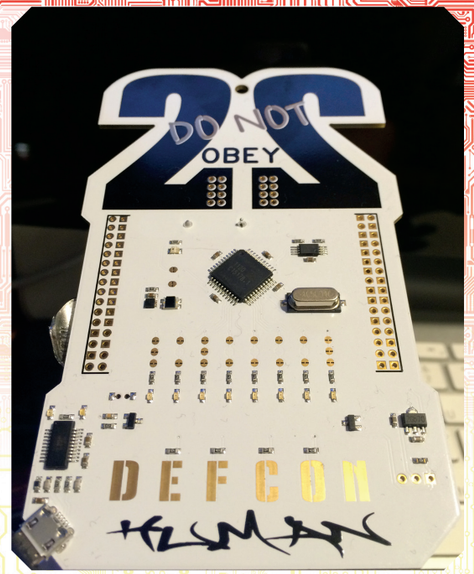
the badge

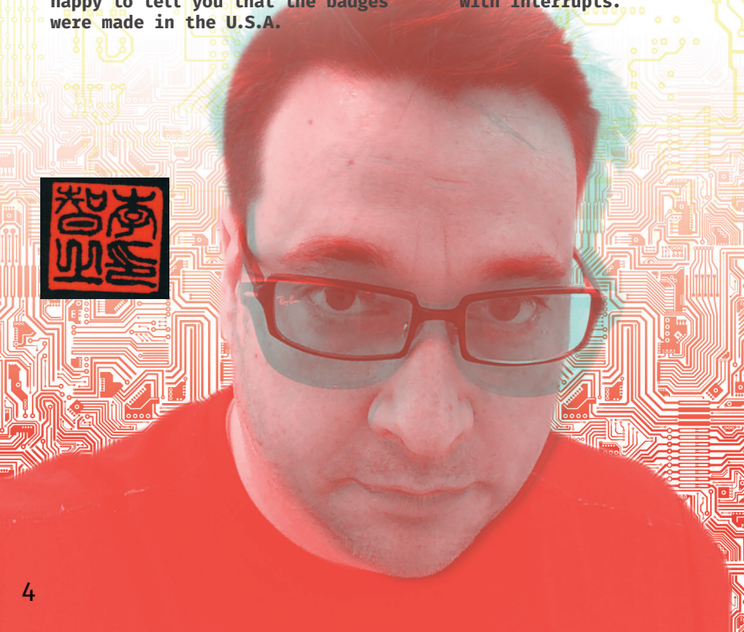
With all of the issues surrounding the badges each year, one might come to believe that there might be a curse. I remember Joe talking about working on the badges on his honeymoon, and not being one to break with tradition I too had the dubious honor of working on the badges on my honeymoon.

eChan and I met through her participation in the MysteryBox challenge (she is a gifted cryptographer and code breaker) so she was very forgiving of the work I had to do on the badges in the midst of the temporal demands a wedding creates. Even so, knowing how busy life would be I called in a huge favor from my longtime friend Jonny Mac, without whose help I would not have made it in time for DEF CON 22. The folks at Parallax (KenG) were also amazing, and I'm happy to tell you that the badges were made in the U.S.A.

The "They Live" theme of this year drove the design and direction we decided to go with the badge.

Every effort was made to encourage experimentation and use of the badge long after the conference ends. The circular pads with center-connecting trace are 'mod-pads', that allow parts to be disconnected from the circuit by cutting the middle with a razor blade, or added back by simply soldering the two pad halves back together. We also went with standard spacing on the breakouts for the I/O to make it easier to create shields, add-ons, and for general use. You can load experimental code to RAM, leaving the EEPROM untouched – so please have a go at changing around the code. Having a multi-core processor on your controller means no fussing with interrupts.





As usual, I can't give away too much – as the badge challenge is an Uber-badge contest – but I do have some cool news – Parallax is announcing that they are open-sourcing the Propeller at DEF CON this year.

We will be awarding prizes for cool and interesting badge hacks, so have fun modding…if you've got something especially neat be sure to stop by the 1o57 room.

Have a great con everyone.

-R.D. "1o57" Clarke

07-21-18-03-18-05-05-22-01-03-14-20-18-06

10-22-25-25-21-18-25-03-12-02-08-19-22-01

17-12-02-08-05-16-14-25-25-22-01-20-15-08

07-17-02-01-07-15-18-17-08-03-18-17-16-08

07-17-02-10-01-07-21-18-10-02-02-17-06-07

21-18-12-15-18-18-05-17-02-06-10-57-10-57

info booth

Are you looking for the latest changes to the schedule? Need to know the scoop? Stop by the Info Booth, located in the Rotunda and the Hallway. We are here to help you enjoy the Con by providing the latest updates and information that is DEF CON. Keep two things in mind...

1) Dumb questions get dumb answers

2) Sometimes we just do not have the answer but we may be able to get it.

For what is happening now and the most up to date schedules visit

http://info.defcon.org/

Here you can download the full updated schedule in multiple formats. During the Con this is the most accurate and current schedule.

services for you:

Directions

Twitter Postings for contests and emergencies

Contest results and updates

Latest Schedule

Program Viewing (or you can earn a program replacement)

Donation point for EFF

Hard Drive dupication of the Media Server content

Humiliation as needed

ALL THE DATA ARE BELONG TO YOU

DEF CON MEDIA SERVER

http://10.0.0.16/

ftp://10.0.0.16/

The DEF CON 22 conference media server has been greatly updated from the past three years. It marks the beginning of "for real" archives and file serving, and currently holds about 10T of data for everyone to download. For speed reasons we are only letting through ftp and http.

NEW THIS YEAR: We have added about 20 security related podcasts, archives of other security conferences, and archives of a few web sites such as cryptome, Guttenberg, gentoomen. We've got the complete Hak5 videos, 2600 Off the Hook, and much more.

To speed things up we are planning a two stage network upgrade. This year we performed step one, going 10Gig in our core switch, firewall, media server, and connections to our aruba wireless controllers. Next year we will do stage two and up the speed of our wireless by upgrading from the exiting 802.11 B/G to B/G/N (And possibly AC) as well as having more tables with irect ethernet switch access for faster downloads.

For those who are interested the media server is running an Intel 1660v2 3.7GHz CPU, 64Gig of ECC 1867MHz RAM, dual LACP bonded 10Gig connections to the core switch. The drive array is running ZFS in a mirror and stripe configuration (Like a RAID 10) of four SAS3 4k 6TB drives for maximum speed in read performance, and there is a crazy Intel PCIe P3700 SSD for an L2ARC read cache. The network will be your bottleneck this year, not the server.

DEF CON MEDIA HARD DRIVE DUPING STATION!

For even faster leeching pleasure we have invested in hard drive duplication towers, and next year I plan to launch the Data Duplication Village.

This year we have three sets of 4TB drives that contain the same data as the media server, just split up and color coded. If you want to duplicate a particular drive you need to show up at the INFO BOOTH with your drives at the start of each day. It will take about 8 hours to dupe a 4TB drive so a set will start in the morning and a set in the evening, to finish overnight.

As of this writing it is sorted like this:

BLUE Drive = Conference Archives 1 of 2, including DEF CON

GREEN Drive = Conference Archives 2 of 2

ORANGE Drive = Podcasts, 1.5T of all Hak5 archives, Cryptome, FOSS Operating Systems, all other content

There will be an updated list at the infobooth.

official DEF CON swag booth

open 8:00 - 18:00
in the Rotunda

DEF CON
BEHIND THE CURTAIN
OFFICE FOR ENTERTAINMENT
REPORT
UNCLASSIFIED

Thursday, August 7th, 2014
20:00-02:00

The following reports detail our findings from investigation into [redacted] auditory experimentation. The committee reports that the following artists have been found to be involved in [redacted] close attention should be paid for [redacted]t tendencies according to DT.

Testing Chamber: Track 1
20:00-21:00 Synnack
21:00-22:00 Texas Noise Factory
** 22:00-23:00 DJ Spooky (That Subliminal Kid) a.k.a. Paul D. Miller **
23:00-00:00 Dee Kaph
00:00-01:00 Alba T. Ross
01:00-02:00 djdead

In accordance with the Protocol 22.A&E for daytime sound subjugation, the committee has contracted SomaFM. All subjects to be subjugated should be relocated to S[redacted] Chamber 2, codenamed "The Chillout Lounge."

Friday, August 8th, 2014
21:00-03:00

Following th[redacted]xperiment, subjects demonstrated signs [redacted]ue. To combat these effects, the research team administered 150 ccs of a[redacted] form of [redacted]y. When subjects came to, many detailed a readiness to "party." The following artists were then prepped for the testing chamber:

Testing Chamber: Track 1
21:00-22:00 CTRL
22:00-22:30 Dual Core
22:30-23:00 YTCracker
** 23:00-00:00 MC Frontalot **
** 00:00-01:00 Anamanaguchi **
01:00-02:00 VJ Q.Alba
02:00-03:00 PyrO

Saturday, August 9th, 2014
21:00-03:00

As expected, subjects described [redacted] testing as "doubleplusgood." One even went as far as to describe it as "tripleplusgood." This subject was rewarded with[redacted]. After the [redacted]g of one subject who called the testing "ungood," Doctors C.AM and Klink declared that a fresh batch of artists should be shipped in for a final session, so that 100% emotional and psychophysical compliance to Protocol 22 could be demonstrated. Procedure was as follows:

Testing Chamber: Track 1
21:00-22:00 Miss DJ Jackalope
22:00-23:00 Floor Kode
** 23:00-00:00 Elite Force **
** 00:00-01:00 the orb **
01:00-02:00 Zebbler Encanti Experience
02:00-03:00 Krisz Klink

contests

Arcade Games + EFF Booth = Awesomesauce

Come play arcade games and talk with EFF staff attorneys, technologists, and activists to discover EFF's latest work defending your freedom online. You can support the growing movement for digital civil liberties and pick up some great EFF gear when you join or renew your membership at special DEF CON rates.

@eff
www.eff.org
Thursday - Saturday 0900 - 1900

Beverage Cooling Contraption Contest

It's our 10 year of BCCC at DEF CON!

Lets face it. Beverages are better when chilled. The Vegas sun can really warm up a beverage. BCCC teams can really cool them down fast! Come watch teams of contraption builders battle for "beverage" chilling glory!

Sure we know how to drink em, but how fast and accurately do you think you can chill them??

Teams will compete by using custom built contraptions with intent to chill "beverages" like they have been doing since 2005. Their contraptions will be tasked with taking an outside temperature beverage (probably 83+ degrees fahrenheit depending on the Las Vegas sun) and chilling it to exactly 46 degrees Fahrenheit this year.

The Beverage Cooling Contraption Contest is always entertaining for both contestants and spectators. Once a beverage has passed through each contraption and been measured for science, it is no longer of use to the contest and becomes waste product. This contest always has plenty of glorious liquid waste product that must be "cleaned" up and "disposed" of. Luckily, there are always many willing contestants and members of the audience to help us with this terrible chore.

Come and join us on the Miranda Patio at 12:00PM on Friday. See teams compete for glory and science!

Friday @ 1200 in Smokers Area

Black Bag

In DEF CONs of yesteryear, attendees witnessed Gringo Warrior... a scenario-based escape game. From the same people who brought you that lockpicking and physical security contest, we now have Black Bag! Instead of merely focusing on your ability to pick locks as you seek an exit, this contest is framed around getting IN and getting back OUT again.

Throughout day one of DEF CON (Friday) you will follow clues and gather intelligence in order to learn details of your target: a rogue covert operative who is staying on-site. The first seven teams of three players each (more than 7 teams might also be possible) to tell us where this target individual can be found will get to participate in the main round the next day.

On Saturday, teams will be tasked with covertly entering the target's room, picking locked cases and cabinets in order to gather intelligence, and then egressing with as much information as possible in under 10 minutes. Expect a variety of real-world physical pen testing tools to make an appearance, and each team will be equipped with a CORE Group / Lares Consulting Red Teamer bag. Follow us on Twitter (@COREblackbag) to stay abreast of all that is planned!

@COREblackbag
Friday 1200 - 1400, Saturday 1300 - 1700

coindroids

It's the year 2014, one year after the robotic uprising. The androids have since learned quite a bit from their once squishy overlords and now conduct war purely with money, specifically the blunt ample currency that is DEFCOIN. Androids, as it turn out, haven't really mastered the art of friendship but have developed quite a fondness for battle.

Battle your way to the top of the leaderboard by attacking rival robots, upgrading your shiny metal ass and finding items to help scattered throughout the conference.

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.

Thursday - Saturday 0900 - 1700

counterfeit badge contest

It's a race against time and competitors to create the most precise counterfeit badge. Use your creativity, cunning, and attention to detail to produce your best duplicate. The winning badge will be auctioned off for Hackers For Charity, bestowing the champion with eternal glory through forgery.

Friday, Saturday 0900 - 2100 Sunday 1000 - 1300 in TE Village

crack me if you can

For the 5th year in a row, Crack Me If You Can returns with the largest password cracking competition in the solar system. Teams across the planet will go head to head once more in the 48 hour fight against sleep and hashes to be crowned the 2014 winners and gain smack talking rights.

Bigger challenges, harder algos, awesome prizes... Fire up the compute clusters, stock up on energy drinks, put the nearest pizza place on speed dial, and stand the hell by for Crack Me If You Can 2014.

At contest start, we will release tens of thousands of passwords hashed with a variety of algorithms, both common and uncommon. Crack as many as you can, more points for harder hashes.

"Pro" and "Street" team compete for a different set of prizes this year. So experts and beginners will have lots of fun.

http://contest.korelogic.com/
Thursday - Saturday 0900 - 2100 Sunday 1000 - 1300

crash and compile

Do you think you can code? Do think you can code while drinking? We're not talking about coding in the warm safe confines of your cubicle. No, this is programming for sport. It's live competition, against the clock, and the other teams. Nine teams believe they have the smarts to solve our programming challenges. Crash and Compile isn't for the weak. It's not just about laying down some sweet sweet code, it's about the style in which you do so. Sound fun? We think it is.

Crash And Compile is a ACM-style programming contest crossed with a drinking game, where teams of two people try to solve as many programming problems as they can. As teams compile and run their programs, each time their code fails to compile, produces the incorrect output or segfaults, the team must drink. Meanwhile, our lovely Team Distraction will be doing what they can to make the job of programming while intoxicated all the more difficult and/or enjoyable.

Saturday @ 1700 on Contest Area Stage

DEFCONBOTS

Contestants will build autonomous robots capable of shooting lasers at moving targets. The targets will move on a track in waves that are increasingly difficult. To win your robot must survive the most number of waves.

Hacker Jeopardy

DEF CON's oldest and most popular contest is back for its 20th running. Beer. Schwag. Adult behavior. Humiliation. Audience participation. You gotta be there!

Friday/Saturday 1930 - 2130 in Track 2

Hacker Jeopardy Trials

We will run two trials to winnow down teams using lightning rounds (no daily doubles, etc.) to validate skills of potential teams BEFORE letting them get on stage.

Thursday - Saturday 1300 - 1530 on Contest Stage

Hacker War Games

Hello Hackers...would you like to play a game? How about a game of "Tactical Ground Warfare"?

Join us out in the desert anytime Aug. 6th (10a - Dusk) or 7th (10a - 12p) before DEF CON starts and test your skills running around a course in the desert shooting a real gun at targets, and at the end a 1 Shot Sniper shot with a bolt action 7.62NATO. If your good enough you may win a FREE badge to DC22 and other prizes.

Every day you test yourself with how good you are with Computer Security threats, but what about testing yourself against Physical Security threats?

Unless otherwise noted, all contests will be held in the Contest area!

Do you have what it takes to be the Ultimate Hacker against both Cyber and Physical Security threats?

TheSiscoCoon on DC Forums
Wednesday 1000 - Dusk / Thursday 1000 - 1200 at DEF CON Shoot Site

hacker pyramid

Come and be a lucky audience member who will participate with a DEF CON Celebrity in a fast paced game of Pyramid! It may be the last Dick Clark property to be Seacrested... so we're bringing it to you FIRST! Every contestant has a chance at the FABULOUS PRIZES - all the way up to the GRAND PRIZE of ?????¢!!!!!!!

Friday / Saturday 2200 - 0000 in Track 2

Hackers Against Humanity

Returning for its second year, Hackers Against Humanity pits contestants with no moral fiber against each other in a battle of the wits! Rules play out just like Cards Against Humanity, only with hacker and DEF CON themed cards. 80 contestants will vie for the ultimate title as "Worse Person Attending DEF CON". A Vegas 2.0 Production

Friday / Saturday 1000 - 1200 on Contest Stage

Hackfortress

Hackfortress by the numbers: It's 30 minutes of non-stop, no holds barred, hacking and Team Fortress 2 action. In those 30 minutes, 6 Tf2players and 4 Hackers will square off against another team of Tf2 players and hackers. Your goal: to score as many points as possible. How do you score points? By solving hack puzzles of all shapes and sizes. Those range from the ridiculous to the obscenely technical. You can also score points in Tf2 by doing what you normally do in that game: Dominate, kill, capture, take revenge. That's not where the fun ends though. Want to block your opponents from submitting a challenge? Want to set them on fire? Of course you do. Who wouldn't? As you accomplish tasks you'll earn coins that can be spent in our "hackconomy". Once the thirty minutes is up, the team with the most points wins.

Friday, Saturday 0900 - 1700 Sunday 1000 - 1300

Network Forensics Puzzle Contest

The International Chess-Boxing Association has recently announced North Korea will be the next host of the ICBA World Cup in 2022. However, recent evidence released by international whistleblower Edward Snowden has potentially uncovered a bribery scandal involving the recently named host and several officials within the ICBA. You have been hired as a forensics investigator, can you identify the bribed officials and the mastermind behind this large scale deception?

Non-Stop - Thursday 1200 - Sunday 1000

openCTF

V&, longtime participants and three time OpenCTF champions, are proud to host the contest for DEF CON 22 - with a totally rad retro theme. If you already have a team, great! If not, you're welcome to play solo, or make some new friends - there will be challenges for all skill levels. Optional pre-registration is available at openctf.com or +1-415-449-4714

Friday, Saturday 1000 - 2100

Pimp my Rascal

Returning for its second year, we set out to challenge your creative side, in style! Why walk the con when you can cruz the halls on a Rascal scooter... Lowered with neon runner lights! Rent a scooter for $60 for 4 days, delivered directly to Rio Hotel, attach and modify scooter until it is the ultimate ride, then stop by the contest area and submit it in the Pimp my Rascal scooter show! Win prizes and the respect of Xzibit all in one contest! A Vegas 2.0 Production

@_vegas20
Thursday - Saturday 0900 - 2100 Sunday 1000 - 1300

project 2 / exploit hackathon

A puzzle contest for individuals or teams (of up to 5) who:

* Lack skill or confidence
* Can't or don't want to put a team together
* Can't or don't want to devote themselves to a contest for the entire con

contests

Unless otherwise noted, all contests will be held in the Contest area!

P2 is a trivia style CTF that consists of a series of puzzles in

several categories to build forensics concepts necessary to do computer forensics. To build concepts & confidence, puzzles start off easy and then become progressively harder. P2 is designed with the novice or first year DEF CON experience in mind.

Unlike other contests, P2 staff wants to assist you in solving puzzles. We focus on experiential learning. We will also be featuring a Metasploit pro-contest for the particularly competitive. But be warned: this contest doesn't play well with others.

Check us out! And bring beer... we get thirsty.

Exploit Hackathon has returned and teamed up with Project 2 to give you two awesome contests in one great space!

What are we going to do to you this year? I'm so glad you asked! We asked for a POC the first year, but you were not ready. Try harder, we said. Last year we told you to hack the Caps Lock away and then gave you a tablet. This year we take hacking back to its community roots. We are going to work with a project that has all our favorite security goodies all in one place; METASPLOIT!

I am bringing my whole bag of of smack as usual. Its about security, its about fun, its about community. We will make you hack, code. You will be JUDGED (and my judges RULE). We will also have our biggest prize EVER! But can you win it?

Thursday - Saturday 0900 - 2100 Sunday 1000 - 1300

scavenger hunt

The strangest, loudest, most chaotic and quite possibly the most infamous game at DEF CON, the Scavenger Hunt! Back once again with a list full of crazy tasks and hard to find items. It's a test of creativity, determination, brains, and above all the hacker mentality.

Thursday - Saturday 0900 - 2100 Sunday 1000 - 1300

schemaverse

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

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

Prizes generally include honorable swag, Bitcoin, software licenses and entire mugs of respect.

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

Thursday - Saturday 0900 - 1800 Sunday 1000 - 1300

social engineer capture the flag

The Social Engineering Capture the flag is a competition that pits an average person against a Fortune 500 Company. Each contestant is given a target company, they had two weeks to build a profile and write a professional report on all OSI on their target... then come to DEF CON and perform a series of LIVE phone calls to their target company to gather as many flags as they can in the time slot they are given.

This year the SECTF brings it back strong with TAG TEAMS! Thats right, you will be partnered with someone you don't know and given a company you don't know and have to gather flags live, in front of hundreds of people. Scared? Good. Now come and have a blast.

Friday, Saturday 1000 - 2000 Sunday 1030 - 1300

sohopelessly broken

Track 0. Pre-con contest. Step 1, identify and exploit 0-day SOHO router vulnerability. Step 2, register to compete. Step 3, demonstrate your exploit at DEF CON. All exploits welcome: full router control, unprivileged/partial control, corruption of internal network, bricking. Prizes. Prestige. Bring it.

Track 1. At-con router-based CTF. Compete to complete over 10 objective-based attack scenarios against semi-vulnerable routers to earn points and dominate. Presented by the EFF

@eff
www.eff.org
WiFi Village Hours

tamper evident contest

This contest evaluates defeats (which gamut from the exceptional to the mundane) primarily against a range of commonly available low to high-level security products. We'll list the exact products in mid June after we've secured everything. The judging system will remain the same with three impartial judges will evaluate each box and score it based off a -1 (No attempt made) to +3 (holy shit without the video and pics we'd never known!) with the possibility of more with a truly Über defeat!

This contest started because Everyday, every one of us comes into contact with many tamper evident technologies. From your groceries and medications, to your postage and home electronics. All too often in the past people have assumed they were safe; that these technologies we're too difficult to defeat or required too much time before someone noticed.

For five years, the DEF CON Tamper Evident contest has been proving that assumption work. Dead wrong.

This team-focused contest includes tapes, seals, locks, tags, even evidence bags amongst other methods where we actively seek out new and exciting methods of defeat.

Friday, Saturday 0900 - 1730 Sunday 1100 - 1300 in HHV/TE Village

TCP/IP drinking game

Back by explicit demand of the maker, TCP/IP drinking game challenges your detailed knowledge of the most prevalent suite of protocols on the Internet! Contestants will be expected to sit on stage, in public forum, and take the most absurd questions about TCP/IP Suite from both the host and visiting questions from the audience. Fail to know a Flag setting? Didn't convert your hex fast enough? Prepare to drink! Presented by Vegas 2.0 and dc303

Friday 1700 on Contest Stage

TD Francis X-Hour film contest

checklist.... camcorder/ smart phone check.. laptop with cheap/free editing software.... check.... 5 buddies to help you make a crazy idea into a 5 minute story telling marvel of science fiction cheeze... Open to all.... Pre-register or register first thing Thursday morning. Get the rules, get your official "I'm making a movie so watch out" orange t-shirt, deal with the monkey wrenches, go out and get it all done in 48 hours or less. Make DEF CON movie making history... Prizes, fame, and fortune await,,, (well a few prizes at least).... Who knows?... maybe the premier of your team's creation will be shown to a captive audience of 8000 hackers and Feds at the DEF CON closing ceremony.... wouldn't that be cool? (oh yeah, associated bragging rights for being the first etc is just one of the great prizes...)

Thursday - Saturday 0900 - 2100

The DEF CON DarkNet Project

Welcome to the DEF CON DarkNet. Our mission is to secure a safe, independent and self-sustaining community free from intrusion and infiltration by those who would enslave us to their own ends. Our opponents are many and they grow ever more modern — spying on us through our information streams and controlling us through messages that we see 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. You will discover hidden messages you would never have noticed and you will accomplish goals you never would have achieved alone. You know that you have what it takes to join us. You'll rise through the ranks as you get your chance to take on the man running the show by using all of the knowledge that you have acquired.

Friday, Saturday 0900 - 2100 Sunday 1000 - 1200

The SECTF4Kids

We have come up with the ultimate treasure hunt for kids ages 6-12. They have to use all their brain power to solve puzzles, crack ciphers, pick locks and race against the clock and other teams to accomplish the tasks given and be crowned the KING or QUEEN of the SECTF4Kids.

Saturday 0900 - 2100 in SECTF Village

warlock gam3z

warl0ck gam3z is a hands-on 24/7; throw-down, no-holds-barred hacker competition focusing on areas of physical security, digital forensics, hacker challenges and whatever craziness our exploit team develops.

This is an online framework so participants can access it regardless of where they are or what network they are connected to via laptop, netbook, tablet or phone.

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

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

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), Lock Picking (onsite) and Flash Challenges. Be careful of the 50/50 Token which may add or subtract points to your score.

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

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

@Gam3z_Inc
https://warl0ck.gam3z.com/defcon
https://www.facebook.com/Gam3zInc
http://www.youtube.com/user/Gam3zInc
Friday, Saturday 0900 - 2100 Sunday 1000 - 1300

wireless capture the flag (WCTF)

The DEF CON 22 WCTF challenges your team to progress through a set of problems and real-life scenarios in the 30MHz - 6GHz range. Like real-world scenarios you will need to break into the network to gain access and once there you become part of the game.

You will demonstrate that you can crack keys, read PCAPs, locate and connect to networks all while decoding signals of interest. Once you have broken into the wireless networks there are further challenges to be discovered. Offense is just as important as defense and your only access is through the air.

Flags will range from pass-phrases, to demodulated signals, to files located on servers and broadcasted through the airwaves.

We will provide periodic updates so make sure you pay attention to what's happening at the WCTF HQ, on twitter, IRC, etc.

http://WCTF.us
@wctf_us
@wifi_Village
Thursday 1400 - 2100, Friday/Saturday 0900 - 2100 Sunday 1000 - 1200

zapping rachel

"Rachel from cardholder services" is the annoying robo-mosquito that has been sucking the blood and mobile minutes of consumers for years. The FTC receives more complaints about voice spam and robocalls than anything else, and complaints about telephony denial of service attacks are growing. The FTC is looking for a next-gen honeypot design to help experts and authorities zap illegal phone spammers and shut down their operations. We'll hold three stand-alone contests Thursday-

Saturday. Winners get cash prizes plus lots of press/kudos/bragging rights. Help zap Rachel like a bug. Full contest rules, judging criteria, and judges list will be available before the contest.

www.ftc.gov
Friday, Saturday 0900 - 2100 Sunday 1000 - 1300

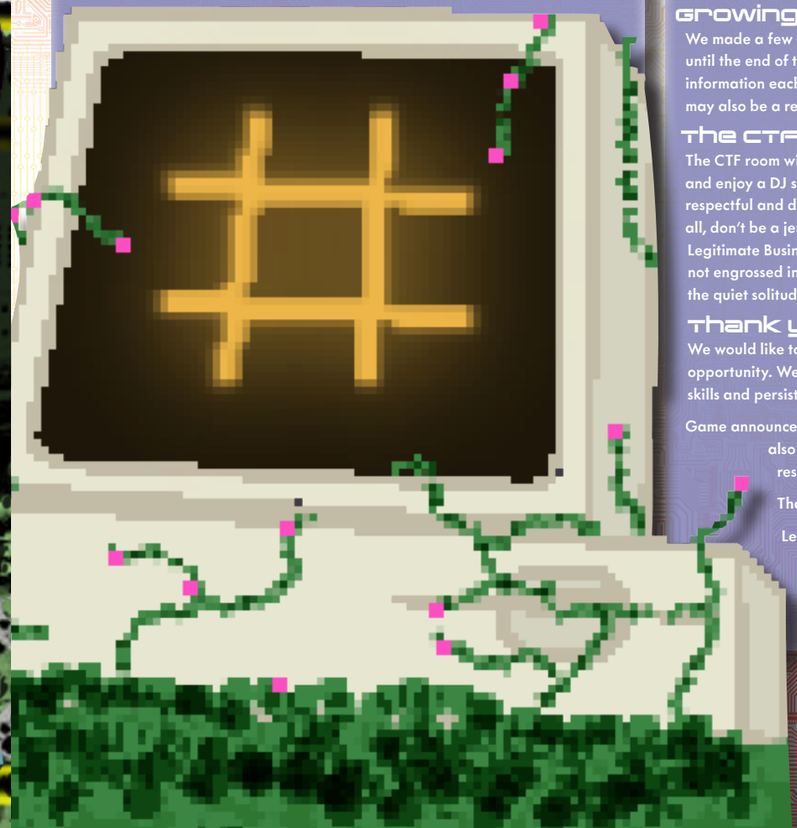
capture the flag

Legitimate Business Syndicate returns to host Capture The Flag at DEF CON 22. We spent the last year figuring out what worked and what didn't, fixed what needed fixing, and built what we were missing.

what is capture the flag?

DEF CON Capture The Flag is a competitive, attackdefense hacking competition. Each team starts with an identical set of network services. Teams use their understanding of these services to attack opponents, while simultaneously defending their own network from other teams. Services may range from a simple mail server to complex virtual machines running invented bytecode.

The scoring system deposits flags in these services and checks for presence of flags on a regular basis. Stealing flags constitutes the offensive aspect of the game. Protecting flags from exfiltration while keeping them available for uptime checks is the defensive aspect.



qualifying competitors

This year's qualification round in May went better than ever!

We had 1,433 teams register (over last year's 898), 4,359 registered players (over last year's 3,108), and harder challenges (look up some of the fantastic writeups from qualifications, especially "dosfun4u").

DEF CON CTF finalists qualify by winning the previous year's finals, placing highly in our qualifying event or by winning one of a select few CTF competitions around the world: Returning champions: Plaid Parliament of Pwning; DEF CON qualifiers, ordered by score: 9447, Reckless Abandon, Routards, raon_ASRT, KAIST GoN, shellphish, CodeRed, HITCON, bluelotus, HackingForChiMac, (Mostly) Men in Black Hats, w3stormz; RuCTFe: More Smoked Leet Chicken; Ghost In The Shellcode: Dragon Sector; Olympic CTF: [SEWorks]penthackon; Boston Key Party: StratumAuhuur; Codegate Finals: Gallopsled; PHDays: ReallyBalalaika; SecuInside qualifiers to be announced.

growing and improving

We made a few adjustments to the scoring system to keep more teams competitive until the end of the game. We will be progressively hiding more scoring information each day, so there may be surprises at closing ceremonies. There may also be a reveal during the competition to keep teams on their toes.

the ctf room

The CTF room will be open for everyone to drop by, watch videos, gawk at teams, and enjoy a DJ set or two throughout the contest. Enjoy yourself, but please be respectful and do not interrupt hackers at work. Do not photograph screens. Above all, don't be a jerk. If you have questions about the contest, talk to a member of Legitimate Business Syndicate. Competitors may be willing to talk when they are not engrossed in the game. Want to experience the CTF action without leaving the quiet solitude of your room? Tune in to DEF CON TV for CTF Highlights!

thank you

We would like to thank CTF competitors around the world for this wonderful opportunity. We would not be able to run this competition without your skills and persistence to inspire us and make it all worthwhile.

Game announcements will be posted to https://twitter.com/legitbs_ctf. We also keep a scoreboard on the wall in the competition room. Final results will be announced during DEF CON closing ceremonies.

Thanks,

Legitimate Business Syndicate

https://legitbs.net

Qualified Teams

Friday Night

Fiders are Spun!

"Fiders are Spun!" hosted by c7five will be throwback to those early DEF CON parties with an eerily similar name. On the docket for the evening are clowns, dancing robots, trick poodles, humans drinking beer, MP3s mixing, Furries, debates in French, sights, sounds and unique smells. By Midnight we are expecting an appearance by Ricardo Montalban, Hervé Villechaize and the rest of the cast from TV's hit show "Fantasy Island" to begin a live reenactment of all 154 episodes (in no particular order).

Hacker Karaoke

Friday and Saturday Night

Do you like music? Do you like performances? Want to BE the performer? Well trot your happy ass down to the fourth annual Hacker Karaoke, DEF CON's on-site karaoke experience where you can be a star, even if you don't know it. Don't want to be a star? At Hacker Karaoke you can also take pride in making an utter fool of yourself. Join us as we put the casbah in "Rock the Casbah".

Hacking, Hip-Hop and Bossa Nova

This event will be the first ever event that mixes hacker culture with Hip Hop and Bossa Nova. It will be legendary. The music will keep everyone on the dance floor. There will also be great activities such as a Tetris Tournament, as well as opportunities to chat with Internet and Cyber Lawyers about pretty much any legal issue under the sun.

Robot Army Art Installation

We've built, and networked, a collective of small delta robots that can either stand alone and perform choreographed movements or be controlled by a user via motion capture (the xbox Kinect or Leap). There will be several motion capture demos that people can use to control the robots... either by dancing or with hand gestures.

Sober Meetup

Not everybody at DEF CON is hammered. We'll give it a second to let that sink in. .... There. Join us for the first ever DEF CON Sober Meetup. So you're not into having your mind altered? Maybe you don't drink because of religious reasons, or at one time you drank a little too much and are now choosing not to, or hell, maybe you just choose not to. No matter what your reasons, come out and join us for a good time and good conversation without the need to tie one on. Lend support to those who need it, and talk about the role alcohol and/or drugs play in the hacker culture and beyond.

Tesla Motors Meet & Greet

Events

4th DEF CON Bike Ride

Dust off your cycling shorts, get out the chamois butter, ice the water, it's almost time for another DEF CON Bike Ride in Las Vegas!

The date of this years bike ride is Aug 7, 2014 at 6am. This is Thursday of DEF CON. We will meet outside the Rio at 5:30am by the valet. There will also be a contingent meeting at the Tuscany at 5:30 am.

http://cycleoverride.org/2014-4th-annual-defcon-bike-ride
Thursday @ 0600 in Rio Valet

Art for charity

Come and see the Art of Eddie Mize (Eddie the y3t1) and help raise money for EFF and HFC.

Contest area hours

Be the Match Registry Drive

Interested in participating in a cool lifehack? When you join the Be The Match Registry® at DEF CON, you become part of every patient's search for a bone marrow donor. Thousands of patients with blood cancers like leukemia and lymphoma, sickle cell and other life-threatening diseases need a bone marrow transplant. You could be the one to save a life.

www.bethematch.org
Friday, Saturday 0900 - 1700 in Contest Area

Beard and Mustache competition

When Whiskers Attack:

The Somethingth Annual DEF CON Beard and Moustache Competition.

This year's Categories are Full Beard, Partial Beard, Moustache only, and freestyle (anything goes, including fake beards).

Our expert panel of judges will once again decide winners in each category based on a wide variety of criteria, including bribes, so fertilize your face and join us for a hairy good time.

Saturday @ 1200 on Contest Area Stage

DEAF CON

DEAF CON is an unofficial, volunteer-run DEF CON event. It is for deaf and deaf-friendly to meet and share thoughts and services.

Besides the meet-up, we bring American Sign Language (ASL) interpreters to the con with funds generated by independent donations. If you would like to request an interpreter, tweet @_DEAFCON_ or visit the Info Booth.

(DEAF CON is NOT affiliated with the speaker-track services using CART and text on screens.)

@_DEAFCON_
Friday @ 1200 in Chill-out Lounge

DEF CON Shoot

The DEF CON Shoot is an opportunity to see and possibly fire 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.

We gather together out in the desert in the days before the start of DEF CON every year and it's always a terrific time for everyone.

Taking place both on the late afternoon of Wednesday and the morning hours of Thursday (with a campout in between for anyone who is so inclined) this is a great way to get yourself some peace and quiet (punctuated by big booms) before the chaos of DEF CON gets fully underway.

If you like guns and want to put tiny holes into lots of things out in the desert, come join us!

Wednesday 1600 CONTINUOUSLY THROUGH Thursday 1300

Faces of DEF CON

Come and meet some of the faces of DEF CON as portrayed by Eddie the y3t1 and stop by and buy some art at the Art for Charity Booth and help raise money for EFF and HFC

Contest area hours

Forum Meet

Totalitarian Dictatorships, Thought Crimes, Total Information Dominance, Massive Surveillance State, They See You, They are Always Watching... Resist, Rebel, Get Reprogrammed, Come join the underground at the DEF CON forum meet.

PS. We're all out of Bubblegum.

WHO: The revolution welcomes all.

WHAT: A chance to meet forum members, new people, party, dance, play a game or two, and have a ball in the ball pit!

WHEN: DEF CON 22, Friday Night 22:00.

WHERE: It's on the Map.

WHY: Free Swag! Games! Ball Pit! Music, with lyrics, that you can dance to! (no techno/skillrex/wubwubwubs)

Hacker Karaoke

Do you like music? Do you like performances? Want to BE the performer? Well trot your happy ass down to the fourth annual Hacker Karaoke, DEF CON's on-site karaoke experience where you can be a star, even if you don't know it. Don't want to be a star? At Hacker Karaoke you can also take pride in making an utter fool of yourself.

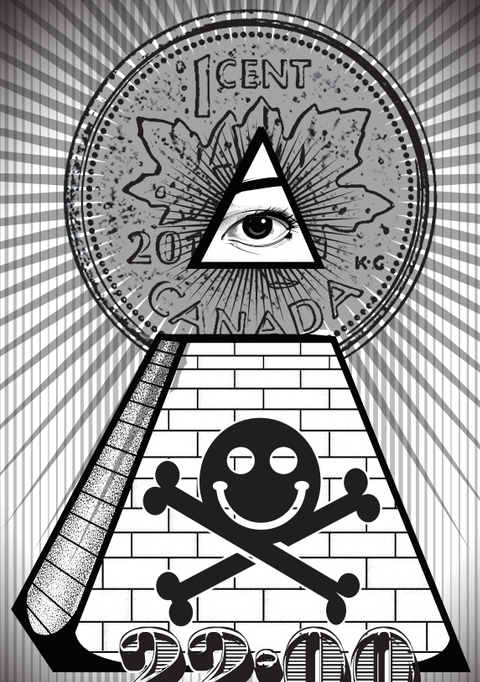
Friday @ 2100 in Pub Crawl (Track 3)

Ham Radio exams

Want to bring back something better from DEF CON than a t-shirt or hangover? Come take the FCC-approved Ham Radio Exams on Sunday, from 12pm-3pm! The exam costs just $15 (cash or check, payable to ARRL; none of it goes to us). If you pass, you'll get an achievement medal and a license good for TEN YEARS to perform ham radio hijinks like transmitting WiFi at 1500W, bouncing signals off the moon, and providing backup communications when the Internet goes down due to malice, disaster, or opinionated squirrel.

http://conham.org
Sunday @ 1200 in Privacy Village

10,000¢ HACKER PYRAMID



22:00

TRACK TWO

FRIDAY & SATURDAY

Come and be a lucky audience member who will participate with a DEF CON Celebrity in a fast paced game of Pyramid! It may be the last Dick Clark property to be Seacrested... so we're bringing it to you FIRST! Every contestant has a chance at the FABULOUS PRIZES ... all the way up to the GRAND PRIZE of 10,000¢

events

Mohawkcon

Get your head buzzed at DEF CON to support the Electronic Frontier Foundation, Hackers For Charity, and your favorite Hackerspaces!

WTF is this all about? We could say we're making a statement about how punk values reflect the fight for digital freedoms, but we'd be full of shit.

We do it because it's fun, and you're all awesome.

@MohawkCon
https://www.facebook.com/MohawkCon
Friday, Saturday 1000 - 1700 @ Contest Area

queercon

Queercon is a group for the LGBT Hackers and those friends of LGBT hackers that just like to have a good time. Social Mixers daily at the Rio and a Queercon Party on Friday night open to all DEF CON hackers that support the LGBT community.

@queercon
http://www.queercon.org/queercon-11/
Friday @ 1600 in iBar

thesummit

This is the world's largest fund raiser for the EFF! After 10 years, we have collected over $175,000! Come be a part of history as we plan to give away over $20K in prizes and door busters to celebrate 10 great years raising awareness and money for the EFF.

theSummit brings together geeky entertainment and the EFF in one magical event you must not miss. Also, rub elbows with our featured guests, 50 of the top speakers from ALL of the security conferences hosted this week in Las Vegas.

For just $50, you get unlimited drinks (until tab runs dry), a chance at raffle prizes, and auction, deep dive into this years hottest talks with the speakers and jam with the best drinking game music known to mankind!

@_vegas20
www.vegassummit.org
Thursday @ 2100 in Chillout Lounge

DEF CON Lawyer Meetup

Oyez, Oyez, Oyez.

Lawyers, Judges, Law Students are admonished to draw near, as the DEF CON Lawyer Meetup will be in session from 4-7pm August 9th in Belize at the Rio. DEF CON General Counsel and Chief Legal Raconteur Jeff McNamara invites all with a connection to the practice of law for a relaxed low-key meet up followed by a spirited trip to the Voodoo Lounge.

Saturday, 4pm to 7pM, in Belize.

villages

crypto and privacy village

For the first time ever, we're having a Crypto and Privacy Village at DEF CON. Here 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 Crypto and Privacy Village will feature workshops on everything from GPG to FOIA, code sprints on security tools, crypto-related games, and talks on privacy from EFF staffers and more.

Friday 1200-1800, saturday 1200-1800

Hardware Hacking village

The HHV has been around since DC16 when Lost and Russ conceived of the idea of bringing hardware to the masses and the HHV has continued to evolve. Besides hosting community soldering stations for badge and kit work we offer talks relating to hardware, mini breakout sessions on a variety of topics and are always there to guide you in finding people that have like interests. Remember you will get the most out of the HHV by talking to people working on projects and sharing ideas.

Thursday - saturday 0900 - 2100, sunday 0900 - 1200

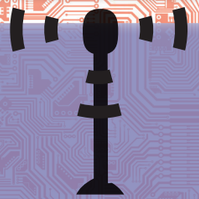
The social engineer village

Born on the back of the Social Engineering Capture the Flag, the SEVillage is the place to talk learn, discuss and engage in all things Social Engineering. This year the SEVillage will contain contests, test of SE-Endurance, the SECTF, the SECTF4Kids as well as a slew of speeches and the 5th anniversary party for SEORG.

Friday, saturday 0900 - 2000, sunday 1000 - 1300

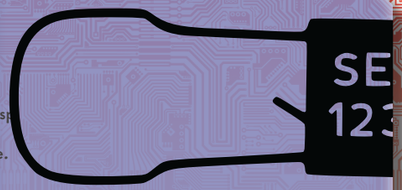
wireless village

The Wireless Village is the place to go to learn about all things related to radio frequency - Wifi, RFID, SDR, Bluetooth, etc. There will be presentations from well known experts in many fields as well as tutorials and question and answer sessions. Meet the authors of your favorite wireless tools! Learn the latest in real world pentesting using wireless from the best and the brightest, this is the place. Be on the cutting edge of wireless – learn how to use your new hackrf or bladerf. We even have training classes so you can get your amateur radio license.



Thursday 1400 - 2100, saturday 0900 - 1200, sunday 1000 - 1300

Tamper Evident Village



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

Friday, saturday 1000 - 2000, sunday 1000 - 1200

Lockpick Village

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

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

Friday, saturday 1000 - 2000, sunday 1000 - 1300

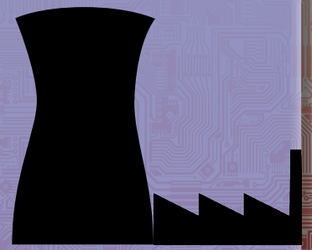
ICS Village

Ever wondered what makes industrial systems tick?

Ever wanted to know how actual logic gets into a programmable logic controller?

Ever wanted to sniff industrial protocols on the network without breaking into your friendly neighborhood factory?

All of the above?! Then welcome to the industrial control systems (ICS) village!



For the first time in DEF CON history, a group of fierce SCADA Ninjas has decided to bring ICS to the DEF CON villages. Unless you are already operating a PLC in your basement hooked up to a water pump or an uranium centrifuge, then this is your best chance to get a kick-start into the world of ICS. The ICS village contains both a full replica of a typical water plant network setup and isolated industrial equipment stations to try out. You may run common security / discovery tools against those systems, program a PLC, use one of our ICS protocol fuzzers or get involved into the development of an open-source ICS honeypot.

We're also planning to bring a number of in-village talks. So see you at DEF CON's first ICS village!

Friday, saturday 0900 - 1700, sunday 1000 - 1200

Packet Hacking Village

The Packet Hacking Village welcomes all DEF CON attendees, for those that are new to DEF CON to the seasoned professionals roaming the halls; there is something for every level of security enthusiast. This village has been created to help enlighten the community through education and awareness. This is where you can find:

The Legendary "Wall of Sheep" which gives attendees a friendly reminder to practice safe computing by using strong end to end encryption. Packet Detective, an education system dedicated to helping attendees start their quest towards a black belt in Packet-Fu. Wi-Fi Sheep Hunt, an exciting wireless competition where anything wireless go's and catching sheep is the goal. Emerging Technology Showcase, an area dedicated to showing off new research, tools and techniques that are used to educate the masses on proper and safe security practices as well as discuss issues/concerns that need to be addressed by vendors. WoSDJCO, listen to some of the hottest DJ's at con spinning for your enjoyment. And... Capture The Packet, the ultimate network forensic been honored by DEF CON as a black badge event four years in a row.

packet detective

Are you interested in learning the art of Network 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 in getting a black belt in Packet-Fu.

emerging technology showcase

The invariable problem with new technologies is the potential for new attack vectors. Some of these present themselves as improper validation checking, poorly designed or implemented protocols or defective products all together. This area of the village is dedicated to showing off new research, tools and techniques that are used to educate the masses on proper and safe security practices as well as discuss issues/concerns that need to be addressed by vendors. This year's focus will be on mobile threats and security.

wifi sheep hunt

Calling all you wireless and RF sniffing packet junkies, you spectrum analyzer gurus, hackers, and those that aren't so-much. The Wifi Sheep hunt is in its third year at DEF CON. This Challenge is DEF CON wide competition so break out your RF gear and start looking for transmitting signals, because if it can transmit RF, it might just be on your quest. Start by obtaining a "Wifi Sheep Hunt License" from the Game Warden at the Wifi Sheep Hunt Table. Solve the encoded riddle, using the license as a map, begin your quest. This challenge requires more than just RF interception, decoding and detection skills, you must be able to exercise your hacking and analytical skills to really put the sheep back in the barn.

capture the packet "ctp"

A game where teams of two compete by monitoring the "live" CTP network traffic in the ultimate network forensics and analysis competition. If you are a Network Samurai who focuses on the defensive arts, this game is for you; there is no attacking. Compete against the best analysts, network engineers and forensic experts in the world by using your Packet FU and analytic skills to beat your opponent and prove you can "Capture The Packet". Contestants will monitor an extremely hostile enterprise class network to look for clues, solve challenges and if they score high enough they may move to the next round. Finals will be held Saturday evening where they have a chance to compete for amazing prizes. If this sounds right up your alley, you can register your team of two on-line at captureThePacket.com or at the CTP table in the Packet Hacking Village. Once you register stay tuned by following our Twitter feed, Facebook page and Web pages for dates and times your team will compete, as well as prizes that will be awarded.

wall of sheep speaker workshops

This year, we have accepted content that focuses primarily on practice and process. The intent is to provide 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 a wide variety of talks for all skill levels!

Topics may include:

Tools on network sniffing, intrusion detection and monitoring, forensics
Tools for data collection (e.g., Yara, Cuckoo Sandbox)
Python & Ruby programming for security practitioners
Hardening the enterprise using open source tools
Getting multi-vendor tools working together
Tool/task automation and optimization
Incident response process and procedures
Thursday - Saturday 0900 - 1900 Sunday 1000 - 1300

ASYLUM

r00tz Asylum is a nonprofit dedicated to teaching kids around the world how to love being white-hat hackers.

A white-hat hacker is someone who enjoys thinking of innovative new ways to make, break and use anything to create a better world.

An asylum is a safe place to learn.

Kids Only - Age 8-16 (Parent Required)
Friday-Sunday 10:00-15:00
Crown Theatre (located on the side of the casino floor)

PRESENTATIONS & WORKSHOPS

From Easter Eggs to Surveillance Systems
- Tom Cross

How to Becoming a Defcoin Millionaire
- Renderman

Hacking the Mars Curiosity Rover
- Don Bailey

Pwning a Google Chromebook
- Matt Moore & Parisa Tabriz

Breaking into Facebwrk and Twitzer
- Sameer Baholtra and Mark Risher

Gathering & Hunting
- Adam Mikrut

The Throwing Star
- Michael Ossmann

Hacking a Living
- Ed Amoroso, Matt Amoroso

Hacking Cars
- Charlie Miller

The Telephone Game
- Meredith Patterson

Breaking World Records
- John, Kevin and James

Fighting Dictators
- Thor Halvorssen

Social Engineering
- Chris Hadnagy

Lockpicking 101
- Deviant

Hacking the Law
- Adi Kamdar

Hardware Hacking
- Joe Grand

Hacker Jeopardy
- Winn & Co.

Meet the Band
- Big Data - Alan Wilkis

CONTESTS

Social Engineering CTF

SaasCrack

Digital Footprints

Name that PLC

Code Breaking

Hacker Jeopardy

Kids Only

DEF CON 101 - The Talk

HighWiz, Lockheed, Pyr0, Roamer, & LosT
10:00 in Track Three

DEF CON 101 is the Alpha to the closing ceremonies' Omega. It's the place to go to learn about the many facets of Con and to begin your Defconian Adventure. Whether you're brand new or a long time attendee, DC101 can start you on the path toward maximizing your DEF CON Experiences.

Protecting SCADA From the Ground Up

AlxRogan (Aaron Bayles)
13:00 in Track Three

Industrial Control Systems (ICS) and SCADA are everywhere, whether you know it or not. Not only do they track flow rates and turn signs for businesses, but they also activate fans and dampers for fire protection and control water distribution in your town. You can't count on ICS and SCADA to be completely off the net anymore, they are being networked internally and Internet-facing more and more. Common Enterprise IT security methods and practices don't fully cover these systems, so come and learn how you should architect and protect the infrastructure that keeps the lights on

AWS for Hackers

Beaker (Seth Van Ommen)
13:00 in DEF CON 101 Track

What tool does every hacker need in their toolset? The entire goddamn giant that is Amazon in their back pocket. AWS is an extremely useful tool for anyone from early noobs just getting their feet wet to seasoned veterans who will become even more kickass. All you need to get started is an internet connection and some keys. Also, CLOUD, there, I said it motherfuckers.

Reverse Engineering Mac Malware

Sarah Edwards, SANS Institute
16:00 in DEF CON 101 Track

Dynamic malware reverse engineering helps forensic analysts and reverse engineers gather quick data points such as callout domains, file download URLs or IP addresses, and dropped or modified files. These methods have long been used on Windows malware...so why not Mac malware? This presentation introduces the audience to methods, tools, and resources to assist reversing Mac binaries with a Mac. Topics include Mach-O file format, virtualization, analysis VM setup, and various analysis tools (native and 3rd-party). This presentation is intended for those familiar with dynamic analysis (with a touch of static thrown in) or for those reverse engineering masters of the Windows executable to get a introductory idea of how to start analyzing Mac malware.

Oh Bother, Cruising The Internet With Your Honeys, Creating Honeynets For Tracking Criminal Organizations

Terrence Garreau & Mike Thompson
16:00 in Track Three

Bandwidth, computing power, and software advancements have empowered hackers to quickly scan for and exploit services across the Internet. While this is a major issue, it does allow researchers to track criminal activity with strategically placed honeypots that lure and trap criminals, allowing organizations to put that information to use improving network security. This talk will outline how to use DDoS vulnerable services to develop a honeypot network that will extract valuable information from the Internet and produce a data feed that can be used to protect online assets with kibana, elasticsearch, logstash, and AMQP.

In the forest of knowledge with 1o57

LosT
15:00 in Track Three

Dashing and daring
Courageous and caring
Faithful and friendly
With stories to share
All through the forest
He sing's out in chorus
Marching along
As his songs fill the air
You best beware
Bouncing here and there and everywhere
High adventure that's beyond compare
LosT will be there
Magic and mystery
Are part of his history
Along with the secret
Of mystery juice
His legend is growing
He takes pride in knowing
He'll fight for what's right
In whatever he'll do

RFIDler: SDR.RFID.FTW

Major Malfunction & Zac Franken
17:00 in Track Three

Software Defined Radio has been quietly revolutionising the world of RF. However, the same revolution has not yet taken place in RFID. The proliferation of RFID/NFC devices means that it is unlikely that you will not interact with one such device or another on a daily basis. Whether it's your car key, door entry card, transport card, contactless credit card, passport, etc. you almost certainly have one in your pocket right now!

RFIDler is a new project, created by Aperture Labs, designed to bring the world of Software Defined Radio into the RFID spectrum. We have created a small, open source, cheap to build platform that allows any suitably powerful microprocessor access to the raw data created by the over-the-air conversation between tag and reader coil. The device can also act as a standalone 'hacking' platform for RFID manipulation/examination. The rest is up to you!

One Man Shop: Building an effective security program all by yourself

Medic (Tim McGuffin)
14:00 in Track Three

At past DEF CON events, including DEF CON 101, most of the attendees we've encountered were either new to the field of security or had security functions in their job description on top of other job duties such as system administration or programming. The purpose of this talk, which is based on real world experiences, is to introduce a multi-year approach to methodologies, techniques, and tools that will allow someone who may be the sole security staff member for an organization to build an effective security program in a cost effective and resource constrained manner. If security is a process, this will provide a "Step 1" to getting that process started.

Data Protection 101 - Successes, Fails, and Fixes

PTzero (Peter Teoh)
10:00 in DEF CON 101 Track

Don't be a Target! How do you protect your organization's data assets? If you're dealing with customers you will likely have their personally identifiable information (PII). Even if you don't have customer data, your HR department will definitely have employees' personal data. What about other sensitive documents like source code, business strategy, etc.?

If you're new to Data Protection (a.k.a. Data Loss Prevention), this presentation will walk you through the basics of how to set up your own successful program. We will also walk through other techniques beyond traditional Data Protection that will enhance your security posture.

Anatomy of a Pentest; Poppin' Boxes like a Pro

PushPin
14:00 in DEF CON 101 Track

Are you excited about hacking and want to be a pentester in the next few years? Let this talk be your guide in understanding what is required to effectively assess a network and all of its associated components. We'll review subjects ranging from assessment toolsets, environment configurations, timelines, what to do when you've accidentally brought down the entire finance department, and how to gently handle the situation when you tell the CIO his baby is ugly.

These techniques and processes can are geared towards to your typical penetration testing processes. The talk has been structured so that not only veterans can benefit from the processes, but the newer/aspiring pentesters can establish a solid foundation for their own work! Hack on.

RF Penetration Testing, Your Air Stinks

RMellendick (Rick Mellendick) & DaKahuna (John Fulmer)
12:00 in DEF CON 101 Track

The purpose of this talk is to discuss the effective radio frequency (RF) tools, tactics, and procedures that we recommend security professionals use when performing a repeatable RF penetration test. This talk will cover the fundamental processes used to identify the RF within the environment, identify the vulnerabilities specific to that environment, and offer attack methodology to exploit those vulnerabilities.

This talk will cover the hardware and software that we recommend for users just starting out all the way from N00bz to l33t hax0rs.

To provide some hands on experience with RF penetration testing, we have developed the Wireless Capture the Flag (WCTF) in the Wireless Village at DEF CON.

We will provide an over view of this contest designed to test your skills, and give you a shooting range to practice and compete, and level of experience doesn't matter, the willingness to learn will get you much further.

Practical Foxhunting 101

Adam Wirth (SimonJ), Communications Systems Engineer, MasterPeace Solutions LTD
11:00 in DEF CON 101 Track

The basic skills needed to quickly locate wireless emitters are easy to learn and no special equipment is required. Despite this, relatively few people have the know-how to put their equipment to work locating emitters as part of penetration testing, RF environment mapping, or tracking their geriatric neighbors using the emanations from their pacemakers. In this talk, you'll learn simple techniques for finding wireless emitters in the environment using readily-available equipment, and how to select and configure foxhunting gear. You'll also get a brief introduction to some more-advanced topics and techniques.

Standing Up an Effective Penetration Testing Team

Wiseacre (Mike Petruzzi)
15:00 in DEF CON 101 Track

Many talks give you information on how to be a better penetration tester. The majority are technical talks on improving techniques or learning new tools. This talk aims to teach the attendees the techniques and pitfalls of putting together a penetration team. It goes beyond identifying the right people to be on the team and the talk explores the concepts of planning, performing and reporting the test. The talk also looks at getting to the root of a client's problem and how to be paid to return.

The Making of DEFCOIN

Xaphan (Jeff Thomas), Beaker (Seth Van Ommen), & Anch (Mike Guthrie)
17:00 in DEF CON 101 Track

If the Juggalos can do it why can't we? We will discuss what it took to create DEFCOIN, the pitfalls we ran into along the way, how many times we had to reset the block chain before release (oops) and even what a block chain and other funny words like that mean. Come learn the basics of crypto-currencies, what they are, how they work and watch us attempt to show how real money and electricity is converted to fake money and heat. http://defcoin.org/ | @defcoin

Paging SDR... Why should the NSA have all the fun?

Xaphan (Jeff Thomas) & n00bz (Jason Malley)
12:00 in Track Three

Remember pagers? Those things the dealers used in the first season of The Wire? Did you know that people still use them? Sure you may have turned off that old pager and put in your desk drawer, but that doesn't mean the back end infrastructure was turned off.

This talk will cover the basics of POCSAG/FLEX decoding using cheap SDR dongles and free software. We will also present examples of the kind of unencrypted data that is still being broadcast through the regional and national pager networks.

Friday Presentations

Welcome, and the Making of the DEF CON 22 Badge

The Dark Tangent, LosT

10:00 in Penn & Teller Theatre

Bypass firewalls, application white lists, secure remote desktops under 20 seconds

Zoltán Balázs, Chief Technology Officer at MRG Effitas

13:00 Track Three

In theory, post-exploitation after having remote access is easy. Also in theory, there is no difference between theory and practice. In practice, there is. Imagine a scenario, where you have deployed a malware on a user's workstation, but the target information is on a secure server accessed via two-factor authentication, with screen access only (e.g. RDP, Citrix, etc.). On top of that, the server runs application white-listing, and only the inbound port to the screen server (e.g. 3389) is allowed through the hardware firewall. But you also need persistent interactive C&C communication (e.g. Netcat, Meterpreter, RAT) to this server through the user's workstation. I developed (and will publish) two tools that help you in these situations. The first tool can drop malware to the server through the screen while the user is logged in. The second tool can help you to circumvent the hardware firewall after we can execute code on the server with admin privileges (using a signed kernel driver). My tools are generic meaning that they work against Windows server 2012 and Windows 8, and they work with RDP or other remote desktops. The number of problems you can solve with them are endless, e.g., communicating with bind-shell on webserver behind restricted DMZ. Beware, live demo and fun included!

The $env:PATH less Traveled is Full of Easy Privilege Escalation Vulns

Christopher Campbell, Security Researcher

12:20 in Track Three

15 years after APT was released for Linux, Microsoft is finally going to ship Windows with a package manager! Windows PowerShell OneGet is the easiest and fastest way to install applications and will be a fundamental part of how Microsoft wants you to administer your enterprise. In this talk we will go over OneGet, Nuget and Chocolatey and observe some of the security problems that will have to be overcome before widespread adoption. We will go over the hundreds of privilege escalation vulnerabilities that were found in the over 1800 unique packages that are already available on the repository server. We will also demo vulnerabilities against one of the package managers and PowerShell itself. Come see how to find third-party privilege escalation bugs at scale with the newest addition to PowerSploit.

The Secret Life of Krbtgt

Christopher Campbell, Security Researcher

17:30 in Track Three

A tale of peril and woe, Krbtgt is the domain account that you just can't quit. Quiet and harmless, it has been with your enterprise since you first installed Active Directory. Although disabled, it has witnessed years of poor configurations, remote code execution vulnerabilities and bad administrator passwords. Come hear Krbtgt's story and see why its days should be numbered. If you don't laugh, you'll cry. This talk is targeted at Windows administrators, penetration testers and incident handlers and will explore why Microsoft's implementation of Kerberos is not the answer to its many credential problems.

Hacking US (and UK, Australia, France, etc.) traffic control systems

Cesar Cerrudo, CTO, IOActive Labs

13:00 in Penn & Teller Theatre

Probably many of us have seen that scene from "Live Free or Die Hard" (Die Hard 4) were the "terrorist hackers" manipulate traffic signals by just hitting Enter key or typing a few keys, I wanted to do that! so I started to look around and of course I couldn't get to do the same, that's too Hollywood style! but I got pretty close. I found some interesting devices used by traffic control systems on important cities such as Washington DC, Seattle, New York, San Francisco, Los Angeles, etc. and I could hack them :) I also found that these devices are also used in cities from UK, France, Australia, China, etc. making them even more interesting. This presentation will tell the whole story from how the devices were acquired, the research, on site testing demos (at Seattle, New York and Washington DC), vulnerabilities found and how they can be exploited, and finally some possible NSA style attacks (or should I say cyberwar style attacks?) Oh, I almost forgot, after this presentation anyone will be able to hack these devices and mess traffic control systems since there is no patch available (sorry didn't want to say 0day ;)) I hope that after this I still be allowed to enter (or leave?) the US

Abuse of Blind Automation in Security Tools

Eric (XlogicX) Davisson, Security Researcher

Ruben Alejandro (chap0), Security Researcher

11:00 in Track Three

It is impossibly overwhelming for security personnel to manually analyze all of the data that comes to them in a meaningful way. Intelligent scripting and automation is key. This talk aims to be a humorous reminder of why the word "intelligent" really matters; your security devices might start doing some stupid things when we feed them.

This talk is about abusing signature detection systems and confusing or saturating the tool or analyst. Some technologies you can expect to see trolled are anti-virus, intrusion detection, forensic file carving, PirateEye (yep), grocery store loyalty cards (huh?), and anything we can think of abusing.

Expect to see some new open-source scripts that you can all use. The presenters don't often live in the high-level, so you may see the terminal, some hex and bitwise maths, raw signatures, and demonstrations of these wacky concepts in action. We don't intend to present dry slides on "hacker magic" just to look 1337. We want to show you cool stuff that we are passionate about, stuff we encourage everyone to try themselves, and maybe inspire new ideas (even if they're just pranks...especially).

Why Don't You Just Tell Me Where The ROP Isn't Suppose To Go

David Dorsey, Lead Security Researcher at Click Security

17:00 in Track Three

Using a ROP chain to bypass operating system defenses is commonplace and detecting this technique while executing is still difficult. This talk will discuss a method built on Intel's dynamic binary instrumentation tool, Pin, to dynamically detect ROP attacks against the Microsoft Windows operating system. The method is designed to detect ROP attacks that use the return instruction and the indirect call instruction. We will discuss how we determine if a return or indirect call is jumping to a valid location. Then we will show examples of the method working, discuss its effectiveness, and its limitations. After the talk, the source code for the pintool will be released.

Steganography in Commonly Used HF Radio Protocols

Paul Drapeau, Principal Security Researcher, Confer Technologies Inc.

Brent Dukes

11:00 in Penn & Teller Theatre

Imagine having the capability to covertly send messages to an individual or a larger audience, without the need for large centralized infrastructure where your message could be observed, intercepted, or tampered with by oppressive governments or other third parties. We will discuss the opportunities and challenges with steganography implementations in widely used amateur radio digital modes, and present a proof of concept implementation of hiding messages within innocuous transmissions using the JT65 protocol. This technique could theoretically be used to implement a low cost, low infrastructure, covert, world wide short message broadcasting or point to point protocol. No messages in codes or ciphers intended to obscure the meaning thereof were actually transmitted over the amateur bands during the creation of this talk.

Saving Cyberspace by Reinventing File Sharing

Eijah

15:00 in Track One

Internet access is a basic human right, due to its unparalleled capacity to deliver content and information. Recently, our right to share files online has been under assault by governments, corporations, and others who fear openness and personal privacy rights. People have been persecuted, fined, and even imprisoned for simply sharing data electronically. As private conversations transition from the home to the web, we're losing our fundamental rights to privacy and personal beliefs.

While many of us believe that information should be and can be freely shared, we are not without blame. As experts in our fields we have at our disposal an arsenal of tools, experience, and technologies to open up the Internet for limitless file sharing without fear of retribution or loss of personal privacy and freedom. Saving cyberspace means that there are times when we need to break the mold of old and stale thinking – creating something new and beautiful that has the power to change the world.

This presentation is a free data manifesto, a historical analysis, and a recipe for creating a new approach to file sharing that's free from snooping, intervention, and interruption from all outside entities. If you've ever been concerned about the risks and insecurity of file sharing, make sure to attend. Understanding our right to share is the first step to changing the world.

Saving the Internet (for the Future)

Jason Healey,Director, Cyber Statecraft Initiative, Atlantic Council

10:00 in Track One

Saving the Internet (for the Future): Last year, the Dark Tangent wrote in the DC XXI program that the "balance has swung radically in favor of the offense, and defense seems futile." It has always been easier to attack than to defend on the Internet, even back to 1979 when it was written that "few if any security controls can stop a dedicated" red team. We all accept this as true but the community rarely ever looks at the longer term implications of what happens to the internet if one side has a persistent advantage year after year, decade after decade. Is there a tipping point where the internet becomes no longer a Wild West but Somalia, a complete unstable chaos where the attackers don't just have an advantage but a long-term supremacy? This talk will look at trends and the role of hackers and security researchers.

What the Watchers See: Eavesdropping on Municipal Mesh Cameras for Giggles (or Pure Evil)

Dustin Hoffman, Senior Engineer, Exigent Systems Inc.

Thomas (TK) Kinsey, Senior Engineer, Exigent Systems Inc.

14:00 in Penn & Teller Theatre

Municipalities across the nation are deploying IP-based 802.11 wireless mesh networks for city-wide services, including cameras and microphones for police monitoring, and remote audio broadcasting. Once deployed, the standards-based nature of these networks make it easy for cash-strapped cities to use them for all manner of other IP-based services too.

In this presentation we examine a deployed and operational municipal mesh network designed by LeverageIS using Firetide hardware and Firetide's proprietary Firetide Mesh (formerly "Automesh") wireless mesh protocol. In the process, we decode the previously undocumented mesh protocol enough to (1) "tune in" to live feeds from the various cameras positioned across the city, just like we were in police headquarters, and (2) inject arbitrary video into these streams. There's a demo site for you to see the municipal camera streams for yourself, and our code is included. We'll cover wireless mesh networks and other basic theory, so no prior technical knowledge is required.

Stolen Data Markets: An Economic and Organizational Assessment

Tom Holt, Associate Professor, Michigan State University

Olga Smirnova, Assistant Professor, Eastern Carolina University

Yi-Ting Chua, Michigan State University

12:00 in Track Two

Since the TJX corporation revealed a massive data breach in 2007, incidents of mass data compromise have grabbed media attention. The substantial loss of customer data and resulting fraud have seemingly become more common, including the announcement of the Target and Neiman Marcus compromises in 2013. As a result, the social and technical sciences are increasingly examining the market for data

resale which is driven in part by these data breaches. This research is increasingly driven by assessments of web forum-based markets with varying depth of content and representativeness. As a result, there is a great deal of speculation about the profit margins and economy for stolen data. Researchers rarely provide metrics for the cost of various products, and some argue that the type of forum analyzed may provide inaccurate data on the costs of information. In fact, Herley and Florencio argue that open forums are largely a lemon market, where advertised costs are low but the risk of loss is quite high. Similarly, there is limited research considering the organizational structure of actors in the marketplace. Some in the media use the terms gangs or mafias to refer to the thieves and data sellers who acquire information, but this may not accurate reflect the realities of the relationships between buyers, sellers, moderators, and others who facilitate transactions.

This presentation will explore the economy and organizational composition of stolen data markets through qualitative and quantitative analyses of a sample of threads from 13 Russian and English language forums involved in the sale of stolen data. We present estimates for the costs of various forms of data, and examine the relationship between various social and market conditions and the advertised price for dumps and other financial data. The findings support the argument that higher risk conditions within a forum are associated with lower prices for data, while more legitimate and organized markets have higher prices. In addition, the organizational composition of the market are explored using a qualitative analysis which finds that the markets are primarily collegial in nature at the individual level, enabling individuals to work together in order to facilitate transactions. There is also a distinct division of labor between participants on the basis of the products sold and skill sets available and some evidence of long-term market stability on the basis of managerial structures and time in operation. Finally, quantitative social network analysis techniques are applied to this sample of forums to assess network density, user centrality, and the resiliency of the network structures observed. The policy implications of this study for consumers, law enforcement, and security analysts will be discussed in depth to provide improved mechanisms for the disruption and takedown of stolen data markets globally.

Extreme Privilege Escalation On Windows 8/UEFI Systems

Corey Kallenberg, MITRE
Xeno Kovah, MITRE
14:00 in Track Three

It has come to light that state actors install implants in the BIOS. Let no one ever again question whether BIOS malware is practical or present in the wild. However, in practice attackers can install such implants without ever having physical access to the box. Exploits against the BIOS can allow an attacker to inject arbitrary code into the platform firmware. This talk will describe two such exploits we developed against the latest UEFI firmware.

The UEFI specification has more tightly coupled the bonds of the operating system and the platform firmware by providing the well-defined "runtime services" interface between the OS and the firmware. This interface is more expansive than the interface that existed in the days of conventional BIOS, which has inadvertently increased the attack surface against the platform firmware. Furthermore, Windows 8 has introduced APIs that allow accessing this UEFI interface from a userland process. Vulnerabilities in this interface can potentially allow a userland process to escalate its privileges from "ring 3" all the way up to that of the platform firmware, which includes permanently attaining control of the very-powerful System Management Mode (SMM).

This talk will disclose two vulnerabilities that were discovered in the Intel provided UEFI reference implementation, and detail the unusual techniques needed to successfully exploit them.

Investigating PowerShell Attacks

Ryan Kazanciyan, Technical Director, Mandiant
Matt Hastings, Consultant, Mandiant
13:00 in DEF CON 101 Track

Over the past two years, we've seen targeted attackers increasingly utilize PowerShell to conduct command-and-control in compromised Windows environments. If your organization is running Windows 7 or Server 2008 R2, you've got PowerShell 2.0 installed (and on Server 2012, remoting is enabled by default!). This has created a whole new playground of attack techniques for intruders that have already popped a few admin accounts (or an entire domain). Even if you're not legitimately using PowerShell to administer your systems, you need to be aware of how attackers can enable and abuse its features.

This presentation will focus on common attack patterns performed through PowerShell - such as lateral movement, remote command execution, reconnaissance, file transfer, etc. - and the sources of evidence they leave behind. We'll demonstrate how to collect and interpret these forensic artifacts, both on individual hosts and at scale across the enterprise. Throughout the presentation, we'll include examples from real-world incidents and recommendations on how to limit exposure to these attacks.

Oracle Data Redaction is Broken

David Litchfield, Security specialist, Datacom TSS
10:00 in Track Three

The Oracle data redaction service is a new feature introduced with Oracle 12c. It allows sensitive data, such as PII, to be redacted or masked to prevent it being exposed to attackers. On paper this sounds like a great idea but in practice, Oracle's implementation is vulnerable to multiple attacks that allow an attacker to trivially bypass the masking and launch privilege escalation attacks.

Dark Mail

Ladar Levison, Founder of Lavabit, LLC
Stephen Watt, Lead Developer, Reference Implementation, Dark Mail
17:00 in Track One

Data privacy and anonymity have long been cornerstone interests of the computer security world, but not particularly important to the general public. News events in the past year have seen the political climate shift radically, and now data privacy has become big business with secure mail solutions being the focal point of this new found attention. Dark Mail is not the only solution in the secure mail space, but just as Lavabit's preoccupation with privacy and user autonomy was a rarity when it started over a decade ago, it hopes once again to push mail security forward into a new frontier. It is Dark Mail's objective to achieve the highest degree of security possible - with the introduction of an interoperable mail protocol as an open standard. To that end, we are publishing documents describing the protocol, along with a reference implementations of the client and server under a free software license. What most of the secure email systems in the privacy race have prioritized in tandem are ease of use for the masses, and cryptographically secure encryption of message contents between a sender and recipient. Additionally, they tend to place trust for private key management and encryption in the hands of the end user, and not the mail server. While this would certainly be an improvement over traditional SMTP, it leaves much to be desired. Where do other solutions fall short? Metadata.

Dark Mail is designed to minimize the leakage of metadata so that ancillary information like subject lines, recipients, and attachments doesn't fall into the hands of curious third parties. That means all information about the mail and its contents are completely opaque to everybody but the parties communicating - including the servers handling the messages in transit. Accomplishing these goals wasn't possible using existing standards, which is why we created a security enhanced flavor of SMTP for mail delivery dubbed DMTP. What separates dmail from competing secure mail designs is the level of security it affords the user while retaining its simplicity of use. We have automated the key management functions, so complex cryptography operations are handled without user interaction. Of equal importance is the need for an implementation that is open to peer review, security audits, and cryptanalysis. Unlike many commercial solutions, dmail isn't tethered to a single centralized provider; instead it offers the ability for anybody to host secure mail services. Like today, users will be able to access their mail from anywhere, using a web client with client-side encryption, or a traditional client application on their mobile or desktop device for an even greater degree of security. An open standard will guarantee that users have the freedom to adopt any dmail-compatible client or server implementation of their choosing. Most attendees of this presentation will be familiar with the curious story of Lavabit's demise. While Lavabit's hosted mail service refused to surrender unfettered access to its users' secrets, this course of action may not be the obvious choice for network administrators placed in similar situations. Most digital surveillance efforts require the service provider to be complicit with the wiretapping requests of law enforcement. Dmail aims to protect messages from surveillance and tampering - whether it be subversive or coerced - by placing that capability beyond the reach of service providers. With dmail the keys belong to the user, and the message decryption occurs on the user's device. Even so, users can choose how much to trust a service provider - with standardized modes that reside at different points along the security vs usability spectrum. After running through an overview of the Dark Internet Mail Environment, this talk will delve into the details, showcasing the new protocols: DMTP and DMAP. Then highlight the schemes used by these protocols to provide automagical encryption and illustrate the mechanisms which have been developed to protect against advanced threats. To close the talk, we will provide a public demonstration of the reference implementation – showing the Volcano client and Magma server in action.

Meddle: Framework for Piggy-back Fuzzing and Tool Development

Geoff McDonald, Anti-Virus Researcher at Microsoft
10:00 in DEF CON 101 Track

Towards simplifying the vulnerability fuzzing process, this presentation introduces a moddable framework called Meddle that can be used to piggy-back on existing application's knowledge of protocol by performing piggy-back fuzzing. Meddle is an open source Windows x86 and x64 user-mode C# application that uses IronPython plugins to provide a familiar interface for fuzzing. Why bother spending time understanding the protocol just to try break it?

Two vulnerability fuzzing attacks using Meddle will be demonstrated - one attacking the open source rdp server XRDP, and the other attacking general driver communications from user-mode processes. Several vulnerabilities found with the XRDP server will be briefly discussed, including two that may be exploited for RCE prior to authentication. These attacks are typically based on a piggy-back application (such as the Remote Desktop Connection Client, mstsc.exe), the piggy-back application performs a benchmarking operation, and then fuzzing begins through a parallel set of the piggy-back instances attacking each event sequentially.

Although originally designed as a vulnerability fuzzing framework, Meddle is well-suited for developing reverse-engineering and malware analysis tools. Two simple tools will be presented based on Meddle, including:

1. A capture tool for communication between usermode processes and kernel mode drivers along with a parser to view the captures in Windows Message Analyzer.

2. Malware sandboxing environment proof-of-concept.

In conclusion, the attendees should be able leave the session with a basic understanding of how to use the Meddle framework as well as their own ideas for tools to develop and targets to attack.

USB for all!

Jesse Michael, Security Researcher
Mickey Shkatov, Security Researcher
11:00 in DEF CON 101 Track

USB is used in almost every computing device produced in recent years. In addition to well-known usages like keyboard, mouse, and mass storage, a much wider range of capabilities exist such as Device Firmware Update, USB On-The-Go, debug over USB, and more. What actually happens on the wire? Is there interesting data we can observe or inject into these operations that we can take advantage of? In this talk, we will present an overview of USB and its corresponding attack surface. We will demonstrate different tools and methods that can be used to monitor and abuse USB for malicious purposes.

ShareEnum: We Wrapped Samba So You Don't Have To

Lucas Morris, Manager, Crowe Horwath
Michael McAtee, Senior Consultant, Crowe Horwath
12:00 in DEF CON 101 Track

CIFS shares can tell you a lot about a network, including file access, local administrator access, password reuse, etc.. Until now most people have relied on add-ons to scanning tools to implement Microsoft's complicated network APIs. Some tools wrap existing clients, such as smbclient, or use RPC calls; however, this is inefficient. What

we need is a scanner that utilizes the closest thing we can get to Microsoft's SMB libraries to scan network shares efficiently and quietly. ShareEnum uses the underlying Samba client libraries to list shares, permissions, and even recurse down file trees gathering information including what is stored in each directory.

An Introduction to Back Dooring Operating Systems for Fun and Trolling

Nemus, Security Researcher
15:00 in DEF CON 101 Track

So you want to setup a back door? Have you ever wondered how its done and what you can do to detect back doors on your network and operating systems? Ever wanted to setup a back door to prank a friend?. This presentations will do just that. We will go over the basics of back doors using SSH, NET CAT, Meterpreter and embedding back doors into custom binaries along with the logistics of accessing them after they are in place.

The NSA Playset: RF Retroreflectors

Michael Ossmann, Great Scott Gadgets
12:00 in Penn & Teller Theatre

Of all the technologies revealed in the NSA ANT catalog, perhaps the most exotic is the use of RF retroreflectors for over-the-air surveillance. These tiny implants, without any power supply, transmit information intercepted from digital or analog communications when irradiated by radio signals from an outside source. This modern class of radar eavesdropping technology has never been demonstrated in public before today. I've constructed and tested my own RF retroreflectors, and I'll show you how they work and how easy they are to build with modest soldering skills. I'll even bring along some fully assembled units to give away. Now you can add RF retroreflectors to your own NSA Playset and play along with the NSA!

DEF CON Comedy Jam Part VII, Is This The One With The Whales?

Panel With: David Mortman, Rich Mogull, Chris Hoff, Dave Maynor, Larry Pesce, James Arlen, Rob Graham, and Alex Rothman Shostack
14:00 in Track Two

Weeeeeeeeee're baaaaaack. Bring out your FAIL. It's the most talked about panel at DEF CON! A standing room only event with a wait list at the door. Nothing is sacred, not the industry, not the audience, not even each other. Last year we raised over $2000 for the EFF and over $5000 over the last 5 years, let's see how much we can raise this year....

Diversity in Information Security

Panel with: Jennifer Imhoff-Dousharm, Sandy "Mouse" Clark, Kristin Paget, Jolly, Vyrus and Scott Martin
17:00 in DEF CON 101 Track

Discussion from the point of view of a diverse panel of leading representatives currently in or thinking of becoming part of the Information Security industry. This panel will give you insight to the evolutionary landscape of diversity in the hacking community. We will present statistical evidence showing the lack of sub-culture representation in the hacking community and while these numbers have been decreasing we can still work to encourage cultural variance. By analyzing how diversity is critical to improving the information security industry we will explore positive approaches to encourage recruiting and retention of deficient subcultures, removing of unconscious bias' and discouraging inclusiveness, and introduce the audience to a wide variety of existing support structures. There will be no witch hunt here, there will be no judgement, only information. All of this and more will be answered with open and honest dialogue into one of the most controversial issues currently within our community.

Ephemeral Communications: Why and How?

Panel with: Ryan Lackey, Jon Callas, Elissa Shevinsky, Nico Sell and Possibly more to come.....
16:00 in Track Two

Ephemeral communications applications are increasingly popular ways, especially among younger users, to communicate online. In contrast to "once it's on the Internet, it's forever", these applications promise to delete information rapidly, or to maintain anonymity indefinitely, lowering inhibitions to share sensitive or personal content. There are several types of these applications, as well as ephemeral or anonymous publication use of mainstream tools, with unique security features and general utility. Key people from the major ephemeral applications will debate where the market is, where it's going, and how these systems can best balance user desires with technical and legal requirements.

Am I Being Spied On? Low-tech Ways Of Detecting High-tech Surveillance

Dr. Phil Polstra, Associate Professor of Digital Forensics, Bloomsburg University of Pennsylvania
15:00 in Penn & Teller Theatre

Is someone spying on you? This talk will present several low-tech ways that you can detect even high-tech surveillance. Topics covered will include: detecting surveillance cameras with your cell phone, signs that you are under physical surveillance, detecting active and passive bugs with low cost devices, and detecting devices implanted inside computers, tablets, and cell phones.

Measuring the IQ of your Threat Intelligence feeds

Alex Pinto, Chief Data Scientist, MLSec Project
Kyle Maxwell, Researcher
11:00 in Track Two

Threat Intelligence feeds are now being touted as the saving grace for SIEM and log management deployments, and as a way to supercharge incident detection and even response practices. We have heard similar promises before as an industry, so it is only fair to try to investigate. Since the actual number of breaches and attacks worldwide is unknown, it is impossible to measure how good threat intelligence feeds really are, right? Enter a new scientific breakthrough developed over the last 300 years: statistics!

This presentation will consist of a data-driven analysis of a cross-section of threat intelligence feeds (both open-source and commercial) to measure their statistical bias, overlap, and representability of the unknown population of breaches worldwide. Are they a statistical good measure of the population of "bad stuff" happening out there? Is there even such a thing? How tuned to your specific threat surface are those feeds anyway? Regardless, can we actually make good use of them even if the threats they describe have no overlap with the actual incidents you have been seeing in your environment?

We will provide an open-source tool for attendees to extract, normalize and export data from threat intelligence feeds to use in their internal projects and systems. It will be pre-configured with current OSINT network feed and easily extensible for private or commercial feeds. All the statistical code written and research data used (from the open-source feeds) will be made available in the spirit of reproducible research. The tool itself will be able to be used by attendees to perform the same type of tests on their own data.

Join Alex and Kyle on a journey through the actual real-world usability of threat intelligence to find out which mix of open source and private feeds are right for your organization.

Detecting and Defending Against a Surveillance State

Robert Rowley, Security Researcher, Trustwave Spiderlabs
13:00 in Track One

This talk is based on semi-recent reported leaks that detail how state-actors could be engaging in surveillance against people they deem as 'threats'. I will cover the basics on what was leaked, and focus the talk on how to detect hardware bugs, implanted radio transceivers, firmware injections, cellular network monitoring, etc...

No need to bring your tin-foil hats though, the discussion here is a pragmatical approach to how to detect such threats and identify if you have been targeted. No blind faith approaches, or attempts to sell any privacy snake oil will be found here.

Acquire Current User Hashes Without Admin Privileges

Anton Sapozhnikov, KPMG
16:00 in Track Three

If an attacker has only user level access to an infected machine inside corporate internal network, that means he or she has quite a limited number of ways to get the password of that user. Already known techniques require additional network access or great amount of luck. Having no access to internal network and absence of admin privileges is a common case during spear phishing attacks and social engineering activities. This talk will cover a brand new technique to grab credentials from a pwned machine even without admins privileges. The technique is possible due to a design flaw in the Windows SSPI implementation. A proof of concept tool will also be presented.

From Raxacoricofallapatorius With Love: Case Studies In Insider Threat

Tess Schrodinger
17:00 in Track Two

Espionage, honey pots, encryption, and lies. Clandestine meetings in hotels. The naïve girl seduced by a suave businessman. The quiet engineer who was busted by the shredded to do list found in his trash. Encryption the NSA couldn't crack. What motivates insiders to become threats? How were they caught? What are potential red flags to be aware of? Acquire a new awareness around what makes these people tick.

Veil-Pillage: Post-exploitation 2.0

Will Schroeder, Security Researcher, Veris Group
15:00 in Track Three

The Veil-Framework is a project that aims to bridge the gap between pentesting and red team toolsets. It began with Veil-Evasion, a tool to generate AV-evading payload executables, expanded into payload delivery with the release of Veil-Catapult, and branched into powershell functionality with the release of Veil-PowerView for domain situational awareness. This talk will unveil the newest additional to the Veil-Framework, Veil-Pillage, a fully-fledged, open-source post-exploitation framework that integrates tightly with the existing framework codebase.

We'll start with a quick survey of the post-exploitation landscape, highlighting the advantages and disadvantages of existing tools. We will cover current toolset gap areas, and how the lack of a single solution with all the options and techniques desired drove the development of Veil-Pillage. Major features of the framework will be quickly detailed, and the underlying primitives that modules build on will be explained.

Veil-Pillage, released immediately following this presentation, makes it easy to implement the wealth of existing post-exploitation techniques out there, public or privately developed. Currently developed modules support a breadth of post-exploitation techniques, including enumeration methods, system management, persistence tricks, and more. The integration of various powershell post-exploitation components, assorted methods of hashdumping, and various ways to grab plaintext credentials demonstrate the operational usefulness of Veil-Pillage. The framework utilizes a number of triggering mechanisms with a preference toward stealth, contains complete command line flags for third-party integration, and has comprehensive logging and cleanup script capabilities. Welcome to Veil-Pillage: Post-Exploitation 2.0.

Blinding The Surveillance State

Christopher Soghoian, Principal Technologist, American Civil Liberties Union
16:00 in DEF CON 101 Track

We live in a surveillance state. Law enforcement and intelligence agencies have access to a huge amount of data about us, enabling them to learn intimate, private details about our lives. In part, the ease with which they can obtain such information reflects the fact that our laws have failed to keep up with advances in technology. However, privacy enhancing technologies can offer real protections even when the law does not. That intelligence agencies like the NSA are able to collect records about every telephone call made in the United States, or engage in the bulk surveillance of Internet communications is only possible because so much of our data is transmitted in the clear. The privacy enhancing technologies required to make bulk surveillance impossible and targeted surveillance more difficult already exist. We just need to start using them.

Hacking the FBI: How & Why to Liberate Government Records

Ryan Noah Shapiro, PhD candidate, Massachusetts Institute of Technology
14:00 in Track One

After narrowly avoiding a lengthy activism-related prison sentence, I began PhD work at MIT in part to map out the criminalization of political dissent in Post-9/11 America. Especially in trying to obtain records from the FBI, Freedom

of Information Act (FOIA) work became an essential component of my research. However, it quickly became apparent that the FBI routinely refused to comply with FOIA. Less clear was how the Bureau was managing to accomplish this systematic violation of federal law. Consequently, I spent years using FOIA and other tools to map out the hidden mechanisms of FBI non-compliance with the Freedom of Information Act. It worked. Using the FOIA methodologies I'd developed, I began receiving tens of thousands of pages from the FBI on its targeting of domestic protest groups. As a result, the FBI is now attempting to shut down my research by arguing in court that my dissertation FOIA research itself is a threat to national security.

Such efforts by the FBI are just one component of the ongoing crisis of secrecy we now face. The records of government are the property of the people, but these records are consistently withheld from us. My talk will cover my research into the historical and contemporary use of the rhetoric and apparatus of national security to marginalize political dissent, my work to reveal the hidden mechanisms of FBI FOIA operations, the FBI's efforts to shut down my research, the ongoing crisis of secrecy and consequent threat to democracy, and the pressing need for additional modes of hacking the FBI and other intelligence agencies to pick up where FOIA leaves off. The records of government belong to us. It's time to reclaim them.

The Only Way to Tell the Truth is in Fiction: The Dynamics of Life in the National Security State

Richard Thieme, ThiemeWorks
11:00 in Track One

Over a decade ago, a friend at the National Security Agency told Richard Thieme that he could address the core issues they discussed in a context of "ethical considerations for intelligence and security professionals" only if he wrote fiction. "It's the only way you can tell the truth," he said.

Three dozen published short stories and one novel-in-progress (FOAM) later, one result is "Mind Games," published in 2010 by Duncan Long Publishing, a collection of stories that illuminates "non-consensual realities:" the world of hackers; the worlds of intelligence professionals; encounters with other intelligent life forms; and deeper states of consciousness.

A recent scholarly study of "The Covert Sphere" by Timothy Melley documents the way the growth and influence of the intelligence community since World War 2 has created precisely the reality to which that NSA veteran pointed. The source of much of what "outsiders" believe is communicated through novels, movies, and television programs. But even IC "insiders" rely on those sources as compartmentalization prevents the big picture from coming together because few inside have a "need to know." Thieme asked a historian at the NSA what historical events they could discuss with a reasonable expectation that their words denoted the same details. "Anything up to 1945," the historian said with a laugh – but he wasn't kidding. Point taken.

This fascinating presentation illuminates the mobius strip on which all of us walk as we make our way through the labyrinth of security and intelligence worlds we inhabit of necessity, all of us some of the time and some of us all of the time. It discloses why "post-modernism" is not an affectation but a necessary condition of modern life. It addresses the words of an NSA intelligence analyst who responded to one of Thieme's stories by saying, "most of this isn't fiction, but you have to know which part to have the key to the code." This talk does not provide that key, but it does provide the key to the key. It also throws into relief everything else you hear – whether from the platform or in the hallways – inside this conference. And out there in the "real world." "Nothing is what it seems."

A Journey to Protect Points-of-sale

Nir Valtman, Enterprise Security Architect, NCR Retail
18:00 in Track Two

Many point-of-sale breaches occurred in the past year and many organizations are still vulnerable against the simplest exploits. In this presentation, I explain about how points-of-sale get compromised from both retailer's and software-vendor's perspective. One of the most common threats is memory scraping, which is a difficult issue to solve. Hence, I would like to share with you a demonstration of how it works and what can be done in order to minimize this threat. During this presentation, I will explain the long journey took me to understand how to mitigate it, while walking through the concepts (not exposing vendor names) that don't work and those that can work.

Domain Name Problems and Solutions

Dr. Paul Vixie, CEO, Farsight Security
10:00 in Track Two

Spammers can't use dotted quads or any other literal IP address, since SpamAssassin won't let it through, since it looks too much like spam. So, spammers need cheap and plentiful — dare we say 'too cheap to meter'? — domain names. The DNS industry is only too happy to provide these domain names, cheaply and at massive scale. The end result is that 90% of all domain names are crap, with more on the way. DNS registrars and registries sometimes cooperate with law enforcement and commercial takedown efforts since it results in domains that die sooner thus creating demand for more domains sooner. Spammers and other abusers of the Internet commons sometimes try to keep their domains alive a little longer by changing name server addresses, or changing name server names, many times per day. All of this action and counteraction leaves tracks, and around those tracks, security minded network and server operators can build interesting defenses including DNS RPZ, a firewall that works on DNS names, DNS responses, and DNS metadata; and NOD, a feed of Newly Observed Domains that can be used for brand enforcement, as well as an RPZ that can direct a DNS firewall to treat infant domain names unfairly. Dr. Paul Vixie, long time maintainer of BIND and now CEO of Farsight Security, will explain and demonstrate."

The Open Crypto Audit Project

Kenneth White, Co-Founder, Open Crypto Audit Project
Matthew Green, Research Professor, Johns Hopkins University
16:00 in Track One

Join us for the story of the origins and history of the Open Crypto Audit Project (OCAP). OCAP is a community-driven global initiative which grew out of the first comprehensive public audit and cryptanalysis of the widely used encryption software TrueCrypt®. Our charter is to provide technical assistance to free and open source software projects in the public interest. We serve primarily as a coordinator for volunteers and as a funding mechanism for technical experts in security, software engineering, and cryptography. We conduct analysis and research on FOSS and other widely software, and provide highly specialized technical assistance, analysis and research on free and open source software. This talk will present how we audited TrueCrypt, detailing both the Phase I security assessment, and the Phase II cryptanalysis. Looking forward, in light of GotoFail and HeartBleed, we will discuss future plans for our next audit projects of other open source critical infrastructure.

Practical Aerial Hacking & Surveillance

Glenn Wilkinson, Security Analyst, SensePost
16:00 in Penn & Teller Theatre

The coupling of unmanned aerial vehicles (UAVs) with hacking & surveillance devices presents a novel way to track and profile individuals, as well as attack infrastructure. Whilst there have been numerous stories of stunt-hacking (attaching any existing hack to a flying toy) our research aimed to be practical and add use beyond the capability of ground based units. In this talk we will discuss how people are already and unwittingly being tracked and surveilled by private, law enforcement, and military organizations. We will then present and demonstrate Snoopy, a mass data collection and correlation framework that uses information leaked from the wireless devices that people carry. The framework identifies, tracks, and profiles people by passively collecting wireless information from devices, as well as optionally interrogating devices for further information. We will then discuss the advantages of having Snoopy attached to a UAV and present data and scenarios where altitude and speed are beneficial. Furthermore, we will demonstrate aerial hacking capabilities against both client devices and more generic infrastructure. Expect audience interaction, tool releases, and Snoopy drones / t-shirts / stickers to be handed out for good audience questions.

Client-Side HTTP Cookie Security: Attack and Defense

David Wyde, Software engineer, Cisco
14:00 in DEF CON 101 Track

HTTP cookies are an important part of trust on the web. Users often trade their login credentials for a cookie, which is then used to authenticate subsequent requests. Cookies are valuable to attackers: passwords can be fortified by two-factor authentication and "new login location detected" emails, but session cookies typically bypass these measures. This talk will explore the security implications of how popular browsers store cookies, ways in which cookies can be stolen, and potential mitigations.

From root to SPECIAL: Pwning IBM Mainframes

Philip "Soldier of Fortran" Young
12:00 in Track Three

1.1 million transactions are run through mainframes every second worldwide. From your flight to your ATM withdrawal a mainframe was involved. These critical, mainstays of the corporate IT world aren't going anywhere. But while the hacker community has evolved over the decades, the world of the mainframe security has not.

This talk will demonstrate how to go from meeting an IBM, zSeries z/OS mainframe, getting root and eventually getting system SPECIAL, using tools that exist currently and newly written scripts. It will also show you how you can get access to a mainframe to help develop your own tools and techniques.

This talk will teach you the 'now what' after you've encountered a mainframe, returning the balance from the 'computing mystics' who run the mainframe back to the community.

PoS Attacking the Traveling Salesman

Alex Zacharis
Tsagkarakis Nikolaos, Census
13:00 in Track Two

Our work presents a re-vamped Point-of-Sales (POS) attack targeting the transportation sector and focusing mainly on the international aviation industry. Through a real-life attack and while exposing serious security issues at an International Airport, we are re-introducing the popular PoS attack, focusing on the compromise of sensitive personal data such as travelers' identities and trip information. We will disclose all the technical details and proof-of-concepts of the attack we have performed on a real, widely used system: the WiFi time purchase kiosks located inside an International Airport. We will analyze the repercussions of the attack, focusing on the exposure of sensitive traveler information, along with the ability to perform privileged actions such as cashing out money from the kiosks. Our experience with contacting the airport's security will also be discussed.

Utilizing this attack, our team seized the opportunity to recreate the environment on which it took place in order to test a proof-of-concept malware targeting such PoS infrastucture. A step by step guide of the way our malware, named the "Travelers' Spy", exploits the available kiosk modules will be provided. The web camera and the barcode scanner are some of the modules exploited in a combination with memory scrapping to create a unique targeted malware that attacks travelers. Furthermore, a unique command channel for our malware will be introduced through specially crafted Aztec Code images posing as e-tickets. We will also release a newly developed barcode cloning and fuzzing mobile app for Android devices (the "Aztec Revenge" tool).

The tool implements a number of attacks, from simply cloning stolen e-tickets to issuing commands to our malware. "Aztec Revenge" can also be used by security researchers and penetration testers in order to fuzz barcode scanners and the web services behind them to expose security bugs. Finally, a combined attack using both the "Travelers' Spy" malware and the "Aztec Revenge" tool will be presented.

How To Get Phone Companies To Just Say No To Wiretapping

Phil Zimmermann, President & Co-Founder Silent Circle
12:00 in Track One

Phil is going to talk about his latest projects, which are helping several mobile carriers to provide their customers with wiretap-free phone services. These carriers are breaking ranks with the rest of their industry's century-long culture of wiretapping. When you can get actual phone companies to join in the struggle, you know change is afoot. And yes, Navy SEALS are involved.

SKYTALKS

FRIDAY

9AM TBA

10AM QUADLING
CUSTODIET
THE OPEN SOURCE MSSP FRAMEWORK

11AM TBA

12PM TBA

1PM Y3T1
Y3T1'S MOBILE UBERPWN DROP UNIT OR HOW I LEARNED TO LOVE THE TAB

2PM ROD SOTO
CIVILIANIZATION OF WAR PARAMILITARIZATION OF CYBERSPACE AND ITS IMPLICATIONS FOR CIVILIAN INFORMATION SECURITY PROFESSIONALS

3PM BRENDAN O'CONNOR
YOU ARE NOT A SOLDIER, AND THIS IS NOT A WAR

4PM TBA

5PM "JOHN STEED"
INTERNATIONAL INTRIGUE FOR FUN AND PROFIT

SATURDAY

9AM TBA

10AM JEAN-PHILIPPE AUMASSON
SHA1 BACKDOORING AND EXPLOITATION

11AM PATRICK MCNEIL
HOW TO MAKE MONEY FAST USING A PWNED PBX

12PM ALGORYTHM
FOR A GOOD TIME, CALL...

1PM TBA

2PM TBA

3PM BUG HARDY
BREAKING MIFARE ULTRALIGHT.. OR HOW TO GET FREE RIDES AND MORE

4PM ANCH
SECURITY WITH ANCH: ANOTHER TALK, ANOTHER DRINK.

5PM ROB BIRD
SECURITY'S IN YOUR DNA: USING GENOMICS & BIG DATA FOR SECURITY

SUNDAY

9AM-5PM TBA

SKYTALKS/303 TRACK
(TROPICAL E-H)
SKYTALKS.INFO

meet the cfp review board

Many people help review CFPs, but not all wish to be identified. Only those that do are listed below.

Agent X has been involved since DEF CON 6 he is currently head of Speaker Operations. His staff of hardened goons handles speaker logistics at Con. He's super judgmental, impatient and waiting for you to get to the point of your talk. When not working on DEF CON related stuff he handles security issues for a large telecommunications company, and helps to run Laboratory B, the shire's hacker space.

Marc Rogers AKA "CJ" has been a hacker since the late 80's and a Goon for more than 15 years. These days, for his sins, Marc is DEF CON's Head of Security. Marc has more than 20 years experience working in infosec, much of which he either cant talk about, wont talk about, or simply cant remember. When not appearing at security conferences around the world, Marc can be found breaking things for @Lookout in SF.

Our founder. you can check out his info on the Dark Tangent Page

Dead Addict has been staff at DEF CON since its inception 22 years ago. He has spoken at DEF CON, Black Hat, ShmooCon, Yale Law School, SEC-T, Notacon, Rubicon, as well as private security conferences. He has worked in the computer industry for over 22 years, focusing on security for well over a decade. You can often find him contact juggling, wearing a silly bowler hat, or chainsmoking in the 100 degree heat (sometimes all at once). He will not be upset if you want to buy him a beer.

After being involved since DC9 and leading the magical WiFi efforts from DC13 onwards, efffn accepted the challenge of taking the lead of DEF CON's NOC right after DC20 when Lockheed tricked us in believing he was retiring (and not divorcing) the con. efffn not only speaks WiFi, but is an enthusiast of everything related to InfoSec, having spoken in several security conferences around the globe, and is the co-founder of a couple of security conferences in Brazil.

For the last 20 years or so, he has worked with several networking technologies that are no longer used, web applications, databases, protocol fuzzing and today is the director for Trustwave's SpiderLabs in the LATAM region leading a team of very smart folks. And yes, he really enjoys good craft beers. +++

Grifter has been a DEF CON Goon since DC9. He is currently the Senior Goon in charge of DEF CON Evening Event space and the DEF CON Villages. In previous lives he served as a Security, Vendor, and Skybox Goon, Coordinator of the DEF CON Movie Channel, former Organizer of the Scavenger Hunt, and Administrator of the DEF CON Forums. He birthed the idea of the DEF CON Villages and DC Groups into the world, and he's not sorry about it.

Grifter has spoken at DEF CON numerous times, as well as related Hacker, Security, and Industry conferences. He has co-authored several books on various information security topics, and has somehow found a way to convince people to give him money for what he keeps inside his head.(The technical stuff, not the dirty stuff...yet.) He uses this money to provide food and shelter for his family in Salt Lake City, Utah, where he is an active part of DC801, and a founding member of the 801 Labs hackerspace.

Jay Healey runs a program looking at the overlap between internet security and national security and wrote the first military history of how nations have actually fought over the internet. Since he's in Washington he says "cyber" way more than you're comfortable with and prefers you'll get over that soon.

Jericho is an outspoken security-minded something that got his start in hacking the early 90's. That time has led to building valuable skills such as skepticism and anger management as he moved from auditing your networks to auditing your fanciful ideas about how the industry is great and we're really doing better (we aren't). Attending DEF CON 2 and presenting at subsequent earlier DEF CONs, he is tired of seeing conferences routinely accept bad talks and vowed to help. No degree, no certifications, just the willingness to say things many in this dismal industry are thinking but unwilling to say themselves. He remains a champion of security industry integrity and small misunderstood creatures.

Jennifer Granick is a lawyer. Maybe she's even been your lawyer. When she not telling the feds to get a warrant or go home, she's trying to stop the NSA from spying on us all. You can find her at Stanford Law School's Center for Internet and Society where she is Director of Civil Liberties.

Maximiliano Soler lives in Buenos Aires, Argentina. He currently works as Security Analyst for an International Bank with a strong focus in Penetration Testing and Web Application Security. Maxi has also taken part in many conferences such as Black Hat, OWASP AppSec and EKOParty. He is permanently involved in different open source projects related to Web Application Security. As ToolsWatch Member, he is co-organizer of Black Hat Arsenal and Rooted Warfare.

Between reading and responding to several hundred papers she is often seen trolling the free world and raising a mini-hacker. Nikita is most notably known for a celebrated collection of animated gifs and immeasurable cruelty to tall people. She graduated Teh Junior College, Cum Laude, '69, her most notable honors in "cut & paste". Recently she has joined the ranks of internet thought leader, as she is "both tired of doing real work and incapable of managing others". You can subject yourself to her boring life narration via twitter @niki7a.

Roamer is (as of this writing) the retired Sr. Goon in charge of the DEF CON Vendor Area (let's see how that works out). He has been on DEF CON staff since DEF CON 8. He was the founder of the DEF CON WarDriving contest the first 4 years of it's existence and has also run the slogan contest in the past.

Roamer is the guitarist for the Goon Band, Recognize. Although having no actual skills his ability to drink virtually every Goon and attendee under the table has gained him massive prominence in the scene and elevated him to the lofty station you see him in today. When not "working" at DEF CON he is "working" as the Global Information Security Manager and Sr. Enterprise Architect for Sony PlayStation WorldWide Studios. Twitter: @shitroamersays

For 16 years, Russr has been involved in a number of different areas at the conference, including the vendor area, the contest area, Hardware Hacking Village, and more recently, the DEF CON Documentary. He works for his own company at Peak Security, doing research and fun, smaller projects. Russ also charged into fruitless DEF CON retirement, and remains a loyal dog to the minions of the hacker/maker world. He has 20+ years experience in information security, and had discovered the merits of brewing your own beer. Reviewing the potential talks for "The Con" is its own reward, and he's more likely to see something interesting, than another talk about how to do something completely pointless.

Chris (Suggy) Sumner is a security data nerd at Hewlett-Packard. Outside work he co-founded the not-for-profit Online Privacy Foundation who contribute to the emerging discipline of behavioral residue research within online social networks. He has previously spoken on this area of research at DEF CON and other conferences.

After attending a few years as a human, He started getting more involved with the running of the registration desk until he was 'volunteered' to take charge of it. From 9-20 he watched the lines grow as the numbers of attendees grew year after year. The ever growing challenge of being 'THAT GUY' with the badges, the countless requests for FREE entrance, and the mad amount of physical work involved. TW is a proud member of the Ninja Networks, owns NotTheFed.com and doevil.com. TW has worked 17 years with the same large company doing information security work, changing scope every 5 years or so to keep it fresh. Though he no longer runs registration, he tries to stay active behind the scene with the workings of DEF CON as time allows..

Vyrus is a former CIA Counter-intelligence Officer who was convicted of spying for the Soviet Union in 1994. On his first assignment as a case officer, he was stationed in Ankara, Turkey, where his job was to target Soviet intelligence officers for recruitment. Due to financial problems in his personal life as a result of alcohol abuse and high spending, Vyrus began spying for the Soviet Union in 1985, when he walked into the Soviet Embassy in Washington to offer secrets for money..

A special thanks to HighWiz, for all his help in coordinating our newly Official DEF CON 101 track this year. Now running Thursday through Sunday.

HighWiz aka "The Judge". Master of DEF CON 101, Member of the Tribe, Friend of Dorothy.

The Monkey in the Middle: A pentesters guide to playing in traffic.

Anch (Mike Guthrie)

14:00 in DEF CON 101 Track

Prank your friends, collect session information and passwords, edit traffic as it goes by.. become the Monkey(man)-In-The-Middle and do it all...

This presentation will teach you a penetration testers view of man in the middle (MITM) attacks. It will introduce the tools, techniques and methods to get traffic to your hosts. Demonstrations of the tools and methods involved will be presented. Come learn new and interesting ways to prank your friends, experience the all porn internet (redux), learn what mallory is and how to use it, learn how to direct traffic to your proxy, deal with SSL and certificates in interesting ways, and make sure you go (mostly) undetected.

PropLANE: Kind of keeping the NSA from watching you pee

Rob Bathurst (evilrob), Russ Rogers (russr), Mark Carey (phorkus), and Ryan Clarke (L0stboy)

13:00 in Track One

No one likes to be watched, especially on the Internet. Your Internet...habits are only for you to know, not ISPs, hotels, government agencies, your neighbor, that creepy guy down the street with the cantenna, or anyone else. With your privacy in mind; we've combined two things every good hacker should have, a Propeller powered DEF CON badge (DC XX in our case) and a somewhat sober brain to turn the DC badge (with some modifications) into an inline network encryption device. This modified badge, loving called the PropLANE, will allow you to keep your peer-to-peer network traffic away from the prying eyes of the aforementioned creepy guy down the street and impress all the cool hacker peoples of the gender you prefer.

Getting Windows to Play with Itself: A Hacker's Guide to Windows API Abuse

Brady Bloxham, Principal Security Consultant, Silent Break Security

17:00 in Track Three

Windows APIs are often a blackbox with poor documentation, taking input and spewing output with little visibility on what actually happens in the background. By analyzing (and abusing) the underlying functionality of these seemingly benign APIs, we can effectively manipulate Windows into performing stealthy custom attacks bypassing the latest in protective defenses. In this talk, we'll get Windows to play with itself nonstop while revealing 0day persistence, previously unknown DLL injection techniques, and Windows API tips and tricks that any good penetration tester and/or malware developer should know. :) To top it all off, a custom HTTP beaconing backdoor will be released leveraging the newly released persistence and injection techniques. So much Windows abuse, so little time.

Detecting Bluetooth Surveillance Systems

Grant Bugher, Perimeter Grid

15:00 in DEF CON 101 Track

Departments of Transportation around the United States have deployed "little white boxes" — Bluetooth detectors used to monitor traffic speeds and activity. While they're supposedly anonymous, they detect a nearly-unique ID from every car, phone, and PC that passes by. In this presentation, I explore the documentation on these surveillance systems and their capabilities, then build a Bluetooth detector, analyzer, and spoofer with less than $200 of open-source hardware and software. Finally, I turn my own surveillance system on the DOT's and try to detect and map the detectors.

Summary of Attacks Against BIOS and Secure Boot

Yuriy Bulygin, Chief Threat Architect, Intel Security

Oleksandr Bazhaniuk, Security Researcher, Intel Security

Andrew Furtak, Security Researcher, Intel Security

John Loucaides, Security Researcher, Intel Security

12:00 in Penn & Teller Theatre

A variety of attacks targeting platform firmware have been discussed publicly, drawing attention to the pre-boot and firmware components of the platform such as secure boot, OS loaders, and SMM. Windows 8 Secure Boot provides an important protection against bootkits by enforcing a signature check on each boot component.

This talk will detail and organize some of the attacks and how they work. We will demonstrate a full software bypass of secure boot. In addition, we will describe underlying vulnerabilities and how to assess systems for these issues using chipsec (https://github.com/chipsec/chipsec), an open source framework for platform security assessment. We will cover BIOS write protection, forensics on platform firmware, attacks against SMM, attacks against secure boot, and various other issues. After watching, you should understand how these attacks work, how they are mitigated, and how to test a system for the vulnerability.

The Cavalry Year[0] & a Path Forward for Public Safety

Joshua Corman, CTO, Sonatype

Nicholas J Percoco, VP Strategic Services, Rapid7

10:00 in Penn & Teller Theatre

At DEF CON 21, The Cavalry was born. In the face of clear & present threats to "Body, Mind & Soul" it was clear: The Cavalry Isn't Coming... it falls to us... the willing & able... and we have to try to have impact. Over the past year, the initiative reduced its focus and increased its momentum. With a focus on public safety & human life we did our best "Collecting, Connecting, Collaborating" to ensure the safer technology dependence in: Medical, Automotive, Home Electronics & Public Infrastructure. We will update the DEF CON hearts & minds with lessons learned from our workshops & experiments, successes & failures, and momentum in industry and with public policy makers. Year[0] was encouraging. Year[1] will require more structure and transparency if we are to rise to these challenges... As a year of experimentation comes to an end, we will share where we've been, take our licks, and more importantly outline a path forward...

Hacking 911: Adventures in Disruption, Destruction, and Death

Christian "quaddi" Dameff, MD

Jeff "r3plicant" Tully, MD

Peter Hefley, Senior Manager - Sunera

10:00 in Track Two

Ever wonder what you would do if the people you needed most on the worst day of your entire life just weren't there?

Emergency medical services (EMS) are the safety nets we rely on every day for rapid, life-saving help in the absolute gravest of circumstances, but these services rely on antiquated infrastructures that were outdated twenty years ago with vulnerabilities large enough to drive an ambulance through, little municipal governmental support for improved security, and a severe lack of standardized security protocols.

Join quaddi, r3plicant, and Peter- two MDs and a security pro as they review the archaic nature of the 911 dispatch system and its failure to evolve with a cellular world, the problems that continue to plague smaller towns without the resources of large urban centers, how the mischief of swatting and phreaking can quickly transform into the mayhem of cyberwarfare, and the medical devastation that arises in a world without 911. Addressing these problems is a Herculean task but the alternative is a system susceptible to total ownage at the worst possible time.

How to Disclose an Exploit Without Getting in Trouble

Jim Denaro, CipherLaw

Tod Beardsley, Engineering Manager, Metasploit Project

12:00 in DEF CON 101 Track

You have identified a vulnerability and may have developed an exploit. What should you do with it? You might consider going to the vendor, blogging about it, or selling it. There are risks in each of these options. This session will cover the risks to security researchers involved in publishing or selling information that details the operation of hacks, exploits, vulnerabilities and other techniques. This session will provide practical advice on how to reduce the risk of legal action and suggest several approaches to responsible disclosure.

Just What The Doctor Ordered?

Scott Erven, Founder & President SecMedic, Inc

Shawn Merdinger, Healthcare Security Researcher

13:00 in Track Two

You have already heard the stories of security researchers delivering lethal doses of insulin to a pump, or delivering a lethal shock to a vulnerable defibrillator. But what is the reality of medical device security across the enterprise? Join us for an in-depth presentation about a three-year independent research project, encompassing medical devices across all modalities inside today's healthcare landscape. Think they are firewalled off? Well think again. Scarier yet, many remain Internet facing and are vulnerable to strategic attack with the potential loss for human life. And yes you will be amazed at what we found in just 1 hour! We will prove that an attacker can access medical devices at thousands of healthcare facilities from anywhere in the world with the potential loss of human life.

This discussion will also highlight the fallout from security standards not being a requirement for medical device manufacturers, and our experience in identifying and reporting vulnerabilities. We will provide our insight into what needs to be done for healthcare organizations to respond to the new threat of cyber-attack against medical devices. We are working towards a future where cyber security issues in medical devices are a thing of the past. We will discuss the recent success and traction we have gained with healthcare organizations, federal agencies and device manufacturers in addressing these security issues. The train is now moving, so please join us to find out how you can get involved and make a difference by ensuring patient safety.

Mass Scanning the Internet: Tips, Tricks, Results

Robert Graham, Paul McMillan, and Dan Tentler

10:00 in Track Three

Scanning the net — the entire net — is now a thing. This talk will discuss how to do it, such as how to get an ISP that will allow scanning, tools to do the scanning (such as 'masscan'), tools to process results, and dealing with abuse complaints. We Internet, such as all the SCADA/ICS systems we've found. We've only scratched the surface — the Dark Internet of Things is waiting for more things to be discovered. We expect the audience to have a working knowledge of existing portscanners, namely nmap.

Hack All The Things: 20 Devices in 45 Minutes

CJ Heres, Security Consultant

Amir Etemadieh, Security researcher at Accuvant LABS

Mike Baker, Co-Founder OpenWRT

Hans Nielsen, Senior Security Consultant at Matasano

10:00 in Track One

When we heard "Hack All The Things," we took it as a challenge. So at DEF CON this year we're doing exactly that, we're hacking everything. We've taken all of our previous experience exploiting embedded devices and used it to bring you a presentation filled with more exploits than ever before™. This presentation will feature exploits for over 20 devices including but not limited to TVs, baby monitors, media streamers, network cameras, home automation devices, and VoIP gateways. Gain root on your devices, run unsigned kernels; it's your hardware, it's internet connected, and it's horribly insecure.

We will also be following last year's tradition of handing out free hardware to assist the community in rooting their devices. This year we will have a select number of eMMC adapters for presentation attendees.

Raspberry MoCA - A recipe for compromise

Andrew Hunt, Senior Information Security Engineer, Bechtel

16:30 in Track One

Media over Coax Alliance (MoCA) is a protocol specification to enable assured high-bandwidth connections for the high demands of voice, video, and high-speed data connections – the 'triple play.' Verizon, Cox, Comcast, and many other service providers have adopted MoCA as the de facto networking technology used to provide in-home broadband services. This is accomplished by encapsulating Ethernet protocols over coaxial cabling common to interior television wiring. In this presentation, the vulnerabilities presented by the use of MoCA encapsulation in conjunction with common recommended coaxial wiring

standards are realized with the development of Raspberry MoCA, an embedded device that provides a drop-in, automated exploitation kit which can be installed outside the target structure in less than five minutes, providing remote access and complete control over the connecting LAN.

Girl… Fault-Interrupted.

Maggie Jauregui, Software Security Test Engineer

11:00 in Track Two

GFCI's (Ground Fault Circuit Interrupts) are a practically unnoticeable part of our daily lives, except maybe for when you have to fumble around with the Reset button on your hair dryer to get it to work, of course.

I discovered a way to completely melt (magic smoke demo included!) the GFCI mechanism for several off-the-shelf electro domestics wirelessly using specific RF frequencies. Similarly, I'm able to trip other GFCI's (the type built-in to several apartment/home walls) creating a DoS on running electro domestics.

Electro domestics might not be the worst this vulnerability has to offer, since GFCI's are used on many different types of electronics.

I plan on building a directional antenna to hopefully perform remote electro domestic DoS. I will list all vulnerable patents, my discovered vulnerable products, all applicable frequencies, and all affected switch types (such as AFCI's). I also commit to do responsible disclosure of any sensitive electrical attacks, such as RF interference for equipment upon which people's lives or livelihoods may depend.

Secure Random By Default

Dan Kaminsky, Chief Scientist, White Ops

13:00 in Penn & Teller Theatre

As a general rule in security, we have learned that the best way to achieve security is to enable it by default. However, across operating systems and languages, random number generation is always exposed via two separate and most assuredly unequal APIs — insecure and default, and secure but obscure.

Why not fix this? Why not make JavaScript and PHP and Java and Python and even libc rand() return strong entropy? What are the issues stopping us? Should we just shell back to /dev/urandom, or is there merit to userspace entropy gathering? How does fork() and virtualization impact the question? What of performance, and memory consumption, and headless machines?

Turns out the above questions are not actually rhetorical. Just because a change might be a good idea doesn't mean it's a simple one. This will be a deep dive, but one that I believe will actually yield a fix for the repeated *real world* failures of random number generation systems.

Check Your Fingerprints: Cloning the Strong Set

Richard Klafter (Free), Senior Software Engineer, Optimizely

Eric Swanson (Lachesis), Software Developer

15:30 in Track Two

The web of trust has grown steadily over the last 20 years and yet the tooling that supports it has remained stagnant despite staggering hardware advancement. Choices that seemed reasonable 20 years ago (32bit key ids or even 64bit key ids) are obsolete. Using modern GPUs, we have found collisions for every 32bit key id in the strong set, with matching signatures and key-sizes (e.g. RSA 2048). Although this does not break the encryption the web of trust is built on, it further erodes the usability of the web of trust and increases the chance of human error. We will be releasing the tool we developed to find fingerprint collisions. Vanity GPG key anyone?

Screw Becoming A Pentester - When I Grow Up I Want To Be A Bug Bounty Hunter!

Jake Kouns, CISO, Risk Based Security

Carsten Eiram, Chief Research Officer, Risk Based Security

10:00 in DEF CON 101 Track

Everywhere you turn it seems that companies are having serious problems with security, and they desperately need help. Getting into information security provides an incredible career path with what appears to be no end in sight. There are so many disciplines that you can choose in InfoSec with the fundamental argument being whether you join Team Red or Team Blue. Most people tend to decide on the Red team and that becoming a professional pentester is the way to go, as it is the most sexy (and typically pays well). However, with bug bounties currently being all the rage and providing a legal and legitimate way to profit off vulnerability research, who really wants to be a pentester, when you can have so much more fun being a bug bounty hunter!

Researcher motivation in the old days and options for making money off of vulnerabilities were much different than today. This talk analyzes the history of selling vulnerabilities, the introduction of bug bounties, and their evolution. We cover many facets including the different types of programs and the ranges of money that can be made. We then focus on researchers, who have currently chosen the bug bounty hunter lifestyle and provide details on how to get involved in bug bounty programs, which likely pay the best, and which vendors you may want to avoid. What constitutes a good bug bounty program that makes it worth your time? What do you need to know to make sure that you keep yourself out of legal trouble?

Ultimately, we'll provide thoughts on the value of bug bounties, their future, and if they can be a full-time career choice instead of a more traditional position such as pentesting.

Masquerade: How a Helpful Man-in-the-Middle Can Help You Evade Monitoring.

Ryan Lackey, Founder, CryptoSeal, Inc.

Marc Rogers, Principal Security Researcher, Lookout

The Grugq, Information Security Researcher

14:00 in Track Three

Sometimes, hiding the existence of a communication is as important as hiding the contents of that communication.

While simple network tunneling such as Tor or a VPN can keep the contents of communications confidential, under active network monitoring or a restrictive IDS such tunnels are red flags which can subject the user to extreme scrutiny. Format-Transforming Encryption (FTE) can be used to tunnel traffic within otherwise innocuous protocols, keeping both the contents and existence of the sensitive traffic hidden.

However, more advanced automated intrusion detection, or moderately sophisticated manual inspection, raise other red flags when a host reporting to be a laser printer starts browsing the web or opening IM sessions, or when a machine which appears to be a Mac laptop sends network traffic using Windows-specific network settings.

We present Masquerade: a system which combines FTE and host OS profile selection to allow the user to emulate a user-selected operating system and application-set in network traffic and settings, evading both automated detection and frustrating after-the-fact analysis.

Home Insecurity: No alarms, False alarms, and SIGINT

Logan Lamb, Cyber Security Researcher, Center for Trustworthy Embedded Systems

12:00 in Track One

The marketshare of home security systems has substantially increased as vendors incorporate more desirable features: intrusion detection, automation, wireless, and LCD touchpanel controls. Wireless connectivity allows vendors to manufacture cheaper, more featureful products that require little to no home modification to install. Consumer win, since adding devices is easier. The result: an ostensibly more secure, convenient, and connected home for a larger number of citizens. Sadly, this hypothesis is flawed; the idea of covering a home with more security sensors does not translate into a more secure home. Additionally, the number of homes using these vulnerable systems is large, and the growth rate is increasing producing an even larger problem. In this talk, I will demonstrate a generalized approach for compromising three systems: ADT, the largest home security dealer in North America; Honeywell, one of the largest manufacturers of security devices; and Vivint, a top 5 security dealer. We will suppress alarms, create false alarms, and collect artifacts that facilitate tracking the movements of individuals in their homes.

NinjaTV - Increasing Your Smart TV's IQ Without Bricking It

Felix Leder, Director, malware research, Blue Coat Norway

14:00 in Track One

Smart TVs are growing in popularity. Set-top boxes like Apple TV, Roku, or WD TV can make your "normal" TV "smart" and Smart TVs even smarter. Despite their functionality, they're often missing interesting features, like bit-torrent, VPN and even specific TV channels. This presentation is about how to hack into WD TV set-top boxes and how to add experimental functionality without the risk of bricking it. Whether you want to add exotic TV channels, watch right from bit-torrent, or are crazy enough to do bitcoin mining on your TV – you are in charge. We will demonstrate several methods to become root using everything from remote exploits to hardware hacking. Unfortunately, just becoming root isn't sufficient to make persistent changes. Because stronger modifications put your device at risk of bricking or of losing specific services, you must dig deeper. We are going to present and release our "adjusted" firmware that keeps all the manufacturer's encryption and service DRM keys intact. The firmware is minimally invasive and enables customization without risk. Patching becomes as easy as an SMB software upload. For those who want get deeper and dirtier, we will explain the firmware structure, how to extract the relevant encryption keys, and discuss the protected software modules. This includes a short overview of relevant tools to do hot-patching, live-debugging, and pointers to get started on reverse engineering core applications.

Old Skewl Hacking: Porn Free!

Major Malfunction

18:00 in Track Two

Having cut his teeth (and scarred his mind) on hotel Infra-Red controlled TV systems, spent ten years scanning the skies for 'interesting' satellite feeds, in this, the 3rd in his series of 'Old Skewl Hacking' talks, Major Malfunction once again, and with great personal sacrifice, goes down on/into the depths of late-night terrestrial broadcast television to determine how secure 'Pay Per View' / 'Pay Per Night' systems are, and if Debbie really did 'do' Dallas (she did). With a total disgregard for his own sanity and/or eyesight, he takes one for the team and forces himself through not just one, not just two, but possibly even three whole months/nights/hours of terrible Cockney porn to uncover their darkest secrets (for those wishing to spare themselves from exposure to potentially harmful images from this talk, here's the executive summary: don't spend the £5, they cut out all the pink/good bits. There's better stuff for free on that there Internets).

Parental Advisory: Viewer discretion advised: Nudity, sex (moderate? nasty? who can say?), swearing, bad taste.

DEF CON Kids Advisory: See Above! Get your Mom/Dad to bring you to this one! There will be a live demo. There will be BOOBIES! Anti-Sexism Advisory: Please don't Red Card me! I'm not trying to be a douchebag, but that's what they transmit: BOOBIES!

Health and Safety Advisory: Just say no. Stay away. Really.

Terms & conditions apply. You may be charged for entry. "Porn Free" or "Major Malfunction" will never appear on your bill. Always wipe clean after use.

Instrumenting Point-of-Sale Malware: A Case Study in Communicating Malware Analysis More Effectively

Wesley McGrew, Assistant Research Professor, Mississippi State University

13:00 in DEF CON 101 Track

The purpose of this talk is to promote the adoption of better practices in the publication and demonstration of malware analyses. For various reasons, many popular analyses of malware do not contain information required for a peer analyst to replicate the research and verify results. This hurts analysts that wish to continue to work more in-depth on a sample, and reduces the value of such analyses to those who would otherwise be able to use them to learn reverse engineering and improve themselves personally. This paper and talk proposes that we borrow the concept of "executable research" by supplementing our written analysis with material designed to illustrate our analysis using the malware itself. Taking a step beyond traditional sandboxes to implement bespoke virtual environments and scripted instrumentation with commentary can supplement written reports in a way that makes the analysis of malware more sound and useful to others.

As a case-study of this concept, an analysis of the recent high-profile point-of-sale malware, JackPOS is presented with enough information to replicate the analysis on the provided sample. A captured command-and-control server is included and Python-based harnesses are developed and presented that illustrate points of interest from the analysis by instrumenting the execution of the malware itself.

Attacking the Internet of Things using Time

Paul McMillan, Security Engineer, Nebula

17:00 in Track one

Internet of Things devices are often slow and resource constrained. This makes them the perfect target for network-based timing attacks, which allow an attacker to brute-force credentials one character at a time, rather than guessing the entire string at once. We will discuss how timing attacks work, how to optimize them, and how to handle the many factors which can prevent successful exploitation. We will also demonstrate attacks on at least one popular device. After this presentation, you will have the foundation necessary to attack your own devices, and a set of scripts to help you get started.

Touring the Darkside of the Internet. An Introduction to Tor, Darknets, and Bitcoin

Metacortex, Security Researcher
Grifter, Security Researcher

16:00 in DEF CON 101 Track

This is an introduction level talk. The talk itself will cover the basics of Tor, Darknets, Darknet Market places, and Bitcoin. I will start by giving the audience an overview of Tor and how it works. I will cover entry nodes, exit nodes, as well as hidden services. I will then show how you connect to Tor on both Linux/OSX and Windows and demo it off. Once we are connected to Tor, I am going to show how to find Tor hidden services and then demo off browsing around some marketplaces. Once the audience has a solid grasp on what the market places offer, I am going to start dealing the process of purchasing something off of it. I will cover bitcoin and bitcoin mining. After we know about how bitcoin works, we will cover purchasing items. I will cover purchasing PO Box's and the pickup of packages. Finally I will finish up with some concerns you may want to be aware of and my recommendations to help make the use of TOR, Bitcoin, and Marketplaces more secure.

A Survey of Remote Automotive Attack Surfaces

Charlie Miller, Security Engineer, Twitter
Chris Valasek, Director of Threat Intelligence, IOActive

15:00 in Track One

Automotive security concerns have gone from the fringe to the mainstream with security researchers showing the susceptibility of the modern vehicle to local and remote attacks. A malicious attacker leveraging a remote vulnerability could do anything from enabling a microphone for eavesdropping to turning the steering wheel to disabling the brakes.

Last year, we discussed 2 particular vehicles. However, since each manufacturer designs their fleets differently; analysis of remote threats must avoid generalities. This talk takes a step back and examines the automotive network of a large number of different manufacturers from a security perspective. From this larger dataset we can begin to answer questions like: Are some cars more secure from remote compromise than others? Has automotive network security changed for the better (or worse) in the last 5 years? What does the future of automotive security hold and how can we protect our vehicles from attack moving forward?

Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment

Jesus Molina, Security Consultant

16:00 in Track One

Have you ever had the urge to create mayhem at a hotel? Force every hotel guest to watch your favorite TV show with you? Or wake your neighbors up (all 290 of them!) with blaring music and with their blinds up at 3 AM?

For those with the urge, I have the perfect place for you. The St. Regis ShenZhen, a gorgeous luxury hotel occupying the top 28 floors of a 100 story skyscraper, offers guests a unique feature: a room remote control in the form of an IPAD2. The IPAD2 controls the lighting, temperature, music, do not disturb light, TV, even the blinds and other miscellaneous room actions. However, the deployment of the home automation protocol contained several fatal flaws that allow an arbitrary attacker to control virtually every appliance in the hotel remotely. I discovered these flaws and as a result, I was able to create the ultimate remote control: Switch TV off 1280,1281,1283 will switch off the TV in these three room. The attacker does not even need to be at the hotel – he could be in another country.

This talk provides a detailed discussion of the anatomy of the attack: an explanation of reverse engineering of the KNX/IP home automation protocol; a description of the deployment flaws; blueprints on how to create an Ipad Trojan to send commands outside the hotel; and, of course, solutions to avoid all these pitfall in future deployments. Attendees will gain valuable field lessons on how to improve wide scale home automation architectures and discussion topics will include the dangers of utilizing legacy but widely used automation protocols, the utilization of insecure wireless connection, and the use of insecure and unlocked commodity hardware that could easily be modified by an attacker.

The attack has important implications for large scale home automation applications, as several hotels around the world are beginning to offer this room amenity. The severity of these types of security flaws cannot be understated – from creating a chaotic atmosphere to raising room temperatures at night with fatal consequences – hoteliers need to understand the risks and liabilities they are exposed to by faulty security deployments.

VoIP Wars: Attack of the Cisco Phones

Fatih Ozavci, Senior Security Consultant, Sense of Security

15:00 in Track Three

Many hosted VoIP service providers are using Cisco hosted collaboration suite and Cisco VoIP solutions. These Cisco hosted VoIP implementations are very similar; they have Cisco Unified Communication services, SIP protocol for IP Phones of tenants, common conference solutions, Skinny protocol for compliance, generic RTP implementation, VOSS Solutions product family for management services for tenants. Cisco hosted VoIP implementations are vulnerable to many attacks, including:

- VLAN attacks
- SIP trust hacking
- Skinny based signalling attacks
- Bypassing authentication and authorisation
- Call spoofing
- Eavesdropping
- Attacks against IP Phone management services
- Web based vulnerabilities of the products

The presentation covers Skinny and SIP signalling attacks, 0day bypass technique for call spoofing and billing bypass, LAN attacks against supportive services for IP Phones, practical 0day attacks against IP Phone management and tenant services. Attacking Cisco VoIP services requires limited knowledge today with the Viproy Penetration Testing Kit (written by the presenter). It has a dozen modules to test trust hacking issues, signalling attacks against SIP services and Skinny services, gaining unauthorised access, call spoofing, brute-forcing VoIP accounts and debugging services using as MITM. Furthermore, Viproy provides these attack modules in a penetration testing environment and full integration. The presentation contains live demonstration of practical VoIP attacks and usage of new Viproy modules.

Panel: Ask the EFF: The Year in Digital Civil Liberties

Panel with:
Kurt Opsahl, Deputy General Counsel, Electronic Frontier Foundation
Nate Cardozo, EFF Staff Attorney
Mark Jaycox, EFF Legislative Analyst
Yan Zhu, EFF Staff Technologist
Eva Galperin, EFF Global Policy Analyst

16:00 in Track Two

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 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.

Panel - Surveillance on the Silver Screen - Fact or Fiction?

Nicole Ozer, Technology and Civil Liberties Policy Director, ACLU of California
Kevin Bankston, Policy Director, New America Foundation's Open Technology Institute
Timothy Edgar, Fellow, Watson Institute for International Studies, Brown University

18:00 in Track Three

Join ACLU and others for a fun-filled surveillance tour of the movies - from Brazil to Bourne - to talk about what is still fiction and what is now fact. What is technologically possible? What is legal? And what is happening in the courts, Congress, and in companies and communities to reset the balance between government surveillance and individual liberties.

DEF CON the Mystery, Myth and Legend

Panel

17:00 in DEF CON 101 Track

It's hard to throw a stone these days without hitting a security/hacking conference. But, when every year the Las Vegas Metro SWAT Team stages for an interdiction of your convention, you know you have something "different". From crawling through Air Ducts to surreptitiously "acquiring" telco equipment, these are the stories of DEF CON you don't often hear about. The stories of yesteryear that not only helped shape DEF CON but also the people who make up today's hacker and infosec communities at large. DEF CON is the event that helped spawn a generation of hackers and changed the landscape of information security. So come join us for a trip down memory lane as we reveal some of the secrets and stories of what architected the mystery, myth and legend of the hacker community you see today... Now that the statues of limitation have passed.

Abusing Software Defined Networks

Gregory Pickett, Cybersecurity Operations, Hellfire Security

16:00 in Track Three

Software Defined Networking (SDN) transfers all forwarding decisions to a single controller and provides the network with the same degree of control and flexibility as the cloud. And with all the major vendors onboard, it will soon be supporting networks everywhere. But current implementations are full of weaknesses that could easily turn this utopian dream of the future into a nightmare and leave networks world-wide exposed.

With clear-text wire protocol implementations, little support for switch TLS, no authentication for nodes, poorly conceived rate-limiting features in the controllers, controller APIs that don't require authentication , and back-door netconf access, the leading platforms Floodlight and OpenDaylight, are ripe for attack.

And in this session, using a new toolkit that I developed, I'll demonstrate by showing you how to locate and identify these controllers, impersonate switches to DoS them, and engage their wide-open APIs and backdoors to map the network, locate targets, and control access to the network ... even hide from sensors. But all is not lost, because I'll show how to protect them too. Because dream or nightmare, SDN can make a difference in the real world if we just protect it right.

Secure Because Math: A Deep Dive On Machine Learning-Based Monitoring

Alex Pinto, Chief Data Scientist, MLSec Project

13:00 in Track Three

We could all have predicted this with our magical Big Data analytics platforms, but it seems that Machine Learning is the new hotness in Information Security. A great number of startups with 'cy' and 'threat' in their names that claim that their product will defend or detect more effectively than their neighbour's product "because math". And it should be easy to fool people without a PhD or two that math just works.

Indeed, math is powerful and large scale machine learning is an important cornerstone of much of the systems that we use today. However, not all algorithms and techniques are born equal. Machine Learning is a most powerful tool box, but not every tool can be applied to every problem and that's where the pitfalls lie.

This presentation will describe the different techniques available for data analysis and machine learning for information security, and discuss their strengths and caveats. The Ghost of Marketing Past will also show how similar the unfulfilled promises of deterministic and exploratory analysis were, and how to avoid making the same mistakes again.

Finally, the presentation will describe the techniques and feature sets that were developed by the presenter on the past year as a part of his ongoing research project on the subject, in particular present some interesting results obtained since the last presentation on DEF CON 21, and some ideas that could improve the application of machine learning for use in information security, especially in its use as a helper for security analysts in incident detection and response.

Cyberhijacking Airplanes: Truth or Fiction?

Dr. Phil Polstra, Associate Professor of Digital Forensics, Bloomsburg University of Pennsylvania

Captain Polly, Associate Professor of Aviation, University of Dubuque

12:00 in Track Two

There have been several people making bold claims about the ability to remotely hack into aircraft and hijack them from afar. This talk will take a systematic look at the mechanisms others are claiming would permit such cyberhijacking. Each of the most popular techniques will be examined mythbuster style. Along the way several important aircraft technologies will be examined in detail.

Attendees will leave with a better understanding of ADS-B, ADS-A, ACARS, GPS, transponders, collision avoidance systems, autopilots, and avionics networking and communications. No prior knowledge is assumed for attendees.

The primary presenter is a pilot, flight instructor, aviation professor, aircraft mechanic, aircraft inspector, avionics technician, and plane builder who has also worked on the development of some of the avionics systems found in modern airliners.

The second presenter is a former airline pilot with thousands of hours in airliners who is currently an aviation professor in charge of a simulator program.

Don't DDoS Me Bro: Practical DDoS Defense

Blake Self, Senior Security Architect

Shawn "cisc0ninja" Burrell, SOLDIERX Crew

12:00 in Track Three

Layer 7 DDoS attacks have been on the rise since at least 2010, especially attacks that take down websites via resource exhaustion. Using various tools and techniques - it is possible to defend against these attacks on even a shoestring budget. This talk will analyze and discuss the tools, techniques, and technology behind protecting your website from these types of attacks. We will be covering attacks used against soldierx.com as well as attacks seen in Operation Ababil. Source code will be released for SOLDIERX's own DDoS monitoring system, RoboAmp.

Advanced Red Teaming: All Your Badges Are Belong To Us

Eric Smith, Senior Partner, Principal Security Consultant at LARES

Josh Perrymon, Senior Adversarial Engineer at LARES

15:00 in Penn & Teller Theatre

By definition "Red Teaming" or Red Team testing originated from the military whereby describing a team whose primary objective is to penetrate the security controls of "friendly" institutions while evaluating their security measures. The term is widely used today to describe any form or blend of logical, physical and social based attacks on an organization. Since the early 2000's, LARES' core team members have been presenting on and performing advanced Red Team attacks against all verticals and have a 100% success rate for organizational compromise when performing full scope testing.

Fresh out of the think tank of Layer 8 Labs (the R&D division of LARES) and tested in the streets on numerous engagements, this talk will focus specifically on badge access control systems, inherent flaws in their design and demonstrate direct and blended attacks against them. Live demonstrations will be given to show how these flaws lead to facility and system compromise, even against the most secure access control systems and card types being sold to the market today. Custom built tools by the LARES team members will be demonstrated throughout the talk and an interactive discussion will be held at the end of the presentation to discuss current mitigation strategies and industry needs to thwart these attacks going forward.

The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right

Mark Stanislav, Security Evangelist, Duo Security

Zach Lanier, Sr. Security Researcher, Duo Security

11:00 in Track One

This presentation will dive into research, outcomes, and recommendations regarding information security for the "Internet of Things". Mark and Zach will discuss IoT security failures both from their own research as well as the work of people they admire. Attendees are invited to laugh/cringe at concerning examples of improper access control, a complete lack of transport security, hardcoded-everything, and ways to bypass paying for stuff.

Mark and Zach will also discuss the progress that their initiative, BuildItSecure.ly, has made since it was announced this past February at B-Sides San Francisco. Based on their own struggles with approaching smaller technology vendors with bugs and trying to handle coordinated disclosure, Mark and Zach decided to change the process and dialog that was occurring into one that is inclusive, friendly, researcher-centric. They will provide results and key learnings about the establishment of this loose organization of security-minded vendors, partners, and researchers who have decided to focus on improving information security for bootstrapped/crowd-funded IoT products and platforms.

If you're a researcher who wants to know more about attacking this space, an IoT vendor trying to refine your security processes, or just a consumer who cares about their own safety and privacy, this talk will provide some great insights to all of those ends.

I Hunt TR-069 Admins: Pwning ISPs Like a Boss

Shahar Tal, Security & Vulnerability Research Team Leader, Check Point Software Technologies

11:00 in Track Three

Residential gateway (/SOHO router) exploitation is a rising trend in the security landscape - ever so often do we hear of yet another vulnerable device, with the occasional campaign targeted against specific versions of devices through independent scanning or Shodan dorking. We shine a bright light on TR-069/CWMP, the previously under-researched, de-facto CPE device management protocol, and specifically target ACS (Auto Configuration Server) software, whose pwnage can have devastating effects on critical amounts of users. These servers are, by design, in complete control of entire fleets of consumer premises devices, intended for use by ISPs and Telco providers. or nation-state adversaries, of course (sorry NSA, we know it was a cool attack vector with the best research-hours-to-mass-pwnage ratio). We investigate several TR-069 ACS platforms, and demonstrate multiple instances of poorly secured deployments, where we could have gained control over hundreds of thousands of devices. During the talk (pending patch availability), we will release exploits to vulnerabilities we discovered in ACS software, including RCE on a popular package, leading to ACS (and managed fleet) takeover.

Bug Bounty Programs Evolution

Nir Valtman, Enterprise Security Architect

11:00 in DEF CON 101 Track

Bug bounty programs have been hyped in the past 3 years, but this concept was actually widely implemented in the past. Nowadays, we can see big companies spending a lot of money on these programs, while understanding that this is the right way to secure software. However, there are lots of black spots in these programs which most of you are not aware of, such as handling with black hat hackers, ability to control the testers, etc. Henceforth, this presentation explains the current behaviors around these programs and predicts what we should see in the future.

Impostor – Polluting Tor Metadata

Charlie Vedaa

Mike Larsen

15:00 in Track Two

Just using Tor can bring the cops to your door. While the security community was busy scolding the Harvard bomb threat kid for his poor OPSEC, this ugly revelation was largely ignored.

Malware authors are doing their part to remedy the situation; by adding thousands of infected hosts to the Tor network, they're making Tor traffic more common, and making dragnet investigation techniques less viable.

But the hackers need to step up and help too. By taking advantage of weak detection techniques in security tools, fake Tor traffic can be injected with some simple JavaScript. We'll show how easy it is to fool open source monitoring tools, and present a variety of options for testing your closed source gear.

In this fast-paced talk we'll cover how Tor traffic is detected, how false positives can be generated, and how you can help fight for anonymity on the Internet.

Manna from Heaven: Improving the state of wireless rogue AP attacks

Dominic White, CTO, SensePost,

Ian de Villiers, Senior Analyst, SensePost

16:00 in Penn & Teller Theatre

The current state of theoretical attacks against wireless networks should allow this wireless world to be fully subverted for all but some edge cases. Devices can be fooled into connecting to spoofed networks, authentication to wireless networks can either be cracked or intercepted, and our ability to capture credentials at a network level has long been established. Often, the most significant protection users have are hitting the right button on an error message they rarely understand. Worse for the user, these attacks can be repeated per wireless network allowing an attacker to target the weakest link.

This combination of vulnerable and heavily used communications should mean that an attacker needs just arrive at a location and setup for credentials and access to start dropping from the sky. However, the reality is far from this; karma attacks work poorly against modern devices, network authentication of the weakest sort defeats rogue APs and interception tools struggle to find useful details.

This talk is the result of our efforts to bring rogue AP attacks into the modern age. The talk will provides details of our research into increasing the effectiveness of spoofing wireless networks, and the benefits of doing so (i.e. gaining access). It includes the release of a new rogue access point toolkit implementing this research.

Don't Fuck It Up!

Zoz, Robotics Engineer

11:00 in Penn & Teller Theatre

Online antics used to be all about the lulz; now they're all about the pervasive surveillance. Whether you're the director of a TLA just trying to make a booty call or an internet entrepreneur struggling to make your marketplace transactions as smooth as silk, getting up to any kind of mischief involving electronic communications now increasingly means going up against a nation-state adversary. And if even the people who most should know better keep fucking it up, what does that mean for the rest of us? What do the revelations about massive government eavesdropping and data ingestion mean for people who feel they have a right if not a duty to occasionally be disobedient?

It's time for a rant. Analyzing what is currently known or speculated about the state of online spying through the prism of some spectacular fuckups, this talk offers an amusing introduction to how you can maximize your chances of enduring your freedom while not fucking it up. Learn how not to fuck up covering your tracks on the internet, using burner phones, collaborating with other dissidents and more. If you have anything to hide, and all of us do, pay attention and Don't. Fuck. It. Up!

Weaponizing Your Pets: The War Kitteh and the Denial of Service Dog

Gene Bransfield, Principle Security Engineer at Tenacity Solutions, Inc.

10:00 in Track Two

WarKitteh: In my job I have to deliver frequent Information Security briefings to both technical and non-technical professionals. I noticed that as the material got more technical, I began to lose the non-technical crowd. Therefore, I started including humorous pictures of cats and made the briefings include stories about those cats. This worked, and I soon became notorious for my presentation style. After delivering one of those presentations, an audience member offered to lend me their cat tracking collar. The collar contained a GPS device and a cellular component and would track your cats movements throughout the neighborhood. Me being the guy I am, I thought "All you need now is a WiFi sniffing device and you'd have a War Kitteh." I laughed, and started working on it.

DoS Dog: With apologies to LadyMerlin (who has since blessed the project) I attended Outerz0ne one year and LadyMerlin brought her dog. They had labeled the puppy the "Denial of Service Dog" as the pooch demanded so much attention that it was impossible to complete any task other than petting the dog. I thought that if you loaded a doggie backpack with different equipment (e.g. a Pineapple) you could create a Denial of Service Dog of a different kind.

Through the Looking-Glass, and What Eve Found There

Luca "kaeso" Bruno, Research Engineer, Eurecom
Mariano "emdel" Graziano, Ph.D. Student, Eurecom

11:00 in Track Three

Traditionally, network operators have provided some kind of public read-only access to their current view of the BGP routing table, by the means of a "looking glass".

In this talk we inspect looking glass instances from a security point of view, showing many shortcomings and flaws which could let a malicious entity take control of critical devices connected to them.

In particular, we will highlight how easy it is for a low-skilled attacker to gain access to core routers within multiple ISP infrastructures.

I am a legend: Hacking Hearthstone with machine learning

Elie Bursztein, Security Researcher, Google
Celine Bursztein, Founder, PetSquare

10:00 in Track Three

Want to become a legend at Hearthstone — Blizzard's new blockbuster collecting card game — or simply learn how to play better? Then pull up a chair by the hearth and join us for a talk about Hearthstone mechanics and how to improve your chance of winning using machine learning and data mining. This talk is packed with examples that show how to use the tools that we are releasing at DEF CON.

First, we will show you how to uncover the most undervalued cards by building a pricing model reflecting the cards' abilities. Next we will explain how decks can be optimized by tweaking their mana curve to maximize mana efficiency. Finally, we will cover how to predict with relatively good accuracy what opponents are likely to play turn-by-turn by data-mining game replays and building a predictive model that uses that information.

Even if you've never heard of Hearthstone before (shame on you!), you should still come to the talk. That's because it's fun and the techniques discussed can help you improve your performance on other collectible cards games including Magic.

Dropping Docs on Darknets: How People Got Caught

Adrian Crenshaw, TrustedSec & Irongeek.com

12:00 in DEF CON 101 Track

Most of you have probably used Tor before, but I2P may be unfamiliar. Both are anonymization networks that allow people to obfuscate where their traffic is coming from, and also host services (web sites for example) without it being tied back to them. This talk will give an overview of both, but will focus on real world stories of how people were deanonymized. Example cases like Eldo Kim & the Harvard Bomb Threat, Hector Xavier Monsegur (Sabu)/Jeremy Hammond (sup_g) & LulzSec, Freedom Hosting & Eric Eoin Marques and finally Ross William Ulbricht/"Dread Pirate Roberts" of the SilkRoad, will be used to explain how people have been caught and how it could have been avoided.

NSA Playset: DIY WAGONBED Hardware Implant over I2C

Josh Datko, Founder, Cryptotronix, LLC
Teddy Reed, Security Engineer

11:00 in Track One

In this talk we present an open source hardware version of the NSA's hardware trojan codenamed WAGONBED. From the leaked NSA ANT catalog, WAGONBED is described as a malicious hardware device that is connected to a server's I2C bus. Other exploits, like IRONCHEF, install a software exploit that exfiltrate data to the WAGONBED device. Once implanted, the WAGONBED device is connected to a GSM module to produce the NSA's dubbed CROSSBEAM attack.

We present CHUCKWAGON, an open source hardware device that attaches to the I2C bus. With the CHUCKWAGON adapter, we show how to attach an embedded device, like a BeagleBone, to create your own hardware implant. We show how to add a GSM module to CHUCKWAGON to provide the hardware for the CROSSBEAM exploit. We improve the WAGONBED implant concept by using a Trusted Platform Module (TPM) to protect data collection from the target. The talk will demonstrate how these features can be used for good, and evil!

Elevator Hacking - From the Pit to the Penthouse

Deviant Ollam, The CORE Group
Howard Payne, The CORE Group

15:00 in Track One

Throughout the history of hacker culture, elevators have played a key role. From the mystique of students at MIT taking late-night rides upon car tops (don't do that, please!) to the work of modern pen testers who use elevators to bypass building security systems (it's easier than you think!) these devices are often misunderstood and their full range of features and abilities go unexplored. This talk will be an in-depth explanation of how elevators work... allowing for greater understanding, system optimizing, and the subversion of security in many facilities.

Those who attend will learn why an elevator is virtually no different than an unlocked staircase as far as building security is concerned!

Empowering Hackers to Create a Positive Impact

Keren Elazari

14:00 in Track One

In March 2014 I spoke at the annual TED conference about why hackers are a vital part of the information age. I claimed that the world actually needs hackers, and that they play an important social, political and technology role. At first I thought I will encounter objection, but I found out I was preaching to the choir. Surprisingly,many of the smart, powerful, rich people at TED thought hackers were just great. Then I realized: I was preaching to the WRONG choir. It's the hackers who are the change agents, and the only ones who can make a difference when it comes to the future of the net. That's why this talk will speak to the heart of the hacking community about the practical things hackers can do to create a positive impact on the world. Essentially, it's about being a good hacker while staying out of jail and making the world a better place – with things like community outreach projects, crypto parties, voluntary red teams, responsible disclosure and stopping the spread of FUD.

NSA Playset: PCIe

Joe FitzPatrick, Hardware Security Resources, LLC
Miles Crabill, Security Researcher

14:00 in Track Two

Hardware hacks tend to focus on low-speed (jtag, uart) and external (network, usb) interfaces, and PCI Express is typically neither. After a crash course in PCIe Architecture, we'll demonstrate a handful of hacks showing how pull PCIe outside of your system case and add PCIe slots to systems without them, including embedded platforms. We'll top it off with a demonstration of SLOTSCREAMER, an inexpensive device we've configured to access memory and IO, cross-platform and transparent to the OS - all by design with no 0-day needed. The open hardware and software framework that we will release will expand your NSA Playset with the ability to tinker with DMA attacks to read memory, bypass software and hardware security measures, and directly attack other hardware devices in the system. Anyone who has installed a graphics card has all the hardware experience necessary to enjoy this talk and start playing NSA at home!

Shellcodes for ARM: Your Pills Don't Work on Me, x86

Svetlana Gaivoronski, PhD student, Moscow State University, Russia
Ivan Petrov, Masters student, Moscow State University, Russia

15:00 in Track Three

Despite that it is almost 2014, the problem of shellcode detection, discovered in 1999, is still a challenge for researchers in industry and academia. The significance of remotely exploitable vulnerabilities does not seem to fade away. The number of remotely exploitable vulnerabilities continues to grow despite the significant efforts in improving code quality via code analysis tools, code review, and plethora of testing methods.

The other trend of recent years is the rise of variety of ARM-based devices such as mobile phones, tablets, etc. As of now the total number of ARM-based devices exceeds the number of PCs in times. This trend sometimes is terrifying as people trust almost all aspects of their lives to such digital devices. People care much more about convenience than security of the data. For example, mobile phones now knows our financial information, health records, keeps a lot of other private data. That's why ARM-based systems became a cherry pie for attackers.

There is a variety of shellcode detection methods that work more or less acceptable with x86-based shellcodes. There are even hybrid solutions that combine capabilities of existing approaches. Unfortunately, almost all of them focus on a fixed set of shellcode features, specific for x86 architecture. This work aims to cover this gap.

This work makes the following contributions:

•We provide an analysis of existing shellcode detection methods with regards to their applicability to shellcodes developed for ARM architecture. As a result, we show that most of existing algorithms are not applicable for shellcodes written for ARM. Moreover, the methods that work for ARM shellcodes produce too many false positives to be applicable for real-life network channels and 0-day detection.•

We analyzed available ARM-based shellcodes from public exploit databases, and identified a set of ARM shellcode features that distinguishes them from x86 shellcodes and benign binaries.

•We implemented our detectors of ARM shellcode features as an extension for Demorpheus[1] shellcode detection open-source library. The algorithm used for generation of detectors' topology guarantees the solution to be optimal in terms of computational complexity and false positive rate.

Blowing up the Celly - Building Your Own SMS/MMS Fuzzer

Brian Gorenc, Zero Day Initiative, HP Security Research
Matt Molinyawe, Zero Day Initiative, HP Security Research

13:00 in Track One

Every time you hand out your phone number you are giving adversaries access to an ever-increasing attack surface. Text messages and the protocols that support them offer attackers an unbelievable advantage. Mobile phones will typically process the data without user interaction, and (incorrectly) handle a large number of data types, including various picture, audio, and video formats. To make matters worse, you are relying on the carriers to be your front line of defense against these types of attacks. Honestly, the mobile device sounds like it was custom built for remote exploitation.

The question you should be asking yourself is: How do I find weaknesses in this attack surface? This talk will focus on the "do-it-yourself" aspect of building your own SMS/MMS fuzzer. We will take an in-depth look at exercising this attack surface virtually, using emulators, and on the physical devices using OpenBTS and a USRP. To help ease your entry into researching mobile platforms, we will examine the messaging specifications along with the file formats that are available for testing. The value of vulnerabilities in mobile platforms has never been higher. Our goal is to ensure you have all the details you need to quickly find and profit from them.

Deconstructing the Circuit Board Sandwich: Effective Techniques for PCB Reverse Engineering

Joe Grand aka Kingpin, Grand Idea Studio
13:00 in Track Two

Printed Circuit Boards (PCBs), used within nearly every electronic product in the world, are physical carriers for electronic components and provide conductive pathways between them. Created as a sandwich of alternating copper and insulating substrate layers, PCBs can reveal clues about system functionality based on layout heuristics or how components are interconnected. By accessing each individual copper layer of a PCB, one can reconstruct a complete circuit layout or create a schematic diagram of the design.

In this presentation, Joe examines a variety of inexpensive, home-based solutions and state-of-the-art technologies that can facilitate PCB reverse engineering through solder mask removal, delayering, and non-destructive imaging. The work is based on Joe's Research and Analysis of PCB Deconstruction Techniques project performed as part of DARPA's Cyber Fast Track program.

Burner Phone DDOS 2 dollars a day : 70 Calls a Minute

Weston Hecker, Sr Systems Security Analyst/ Network Security
10:00 in Track One

Phone DDOS research. Current proof of concept is dealing with Samsung SCH-U365 QUALCOMM prepaid Verizon phone custom firmware was written that makes it into an anonymous DOS systems It Does PRL list hopping and several other interesting evasion methods. The new firmware allows two features one, you text it a number and it will spam call that number 70 times a min. till battery dies. All for 2 dollars a day. And second feature is that if a number that is in address book calls it, automatically picks up on speaker phone. Also ways to mitigate this attack with load balancing Call manager and Captcha based systems.

Is This Your Pipe? Hijacking the Build Pipeline.

Kyle Kelley, Developer Support Engineer, Rackspace
Greg Anderson, Software Security Engineer,Rackspace
15:00 in DEF CON 101 Track

As developers of the web, we rely on tools to automate building code, run tests, and even deploy services. What happens when we're too trusting of CI/CD pipelines? Credentials get exposed, hijacked, and re-purposed. We'll talk about how often and what happens when people leak public cloud credentials, how some are protecting themselves using encrypted secrets, how to bypass protections against leaking decrypted secrets and how to turn their Jenkins into your own butler. Come hijack credentials out of repositories, steal hidden and encrypted secrets using builds, and hijack infrastructure via their continuous deployment.

Home Alone with localhost: Automating Home Defense

Chris Littlebury, Senior Penetration Tester, Knowledge Consulting Group, Inc.
13:00 in DEF CON 101 Track

Home automation is everywhere, and so are their exploits. This presentation will go over a brief history of home automation techniques, cover modern technologies used today, detail some of the current exploits used against modern automation and security systems, and give examples on how to defend against them. You'll be provided with the knowledge necessary to build your own home-Skynet system- complete with passive and active defenses against physical and wireless attacks. If you like Raspberry Pis, RF hacks, dirty soldering jobs, and even dirtier code, then this is your talk.

Weird-Machine Motivated Practical Page Table Shellcode & Finding Out What's Running on Your System

Shane Macaulay, Director of Cloud Security, IOActive
13:00 in Track Three

Windows7 & Server 2008R2 and earlier kernels contain significant executable regions available for abuse. These regions are great hiding places and more; e.g. Using PTE shellcode from ring3 to induce code into ring0. Hiding rootkits with encoded and decoded page table entries.

Additional ranges/vectors, Kernel Shim Engine, ACPI/AML, boot-up resources & artifacts will also be shown to be useful for code gadgets.

Understanding the state of affairs with the changes between Win7/8 and what exposures were closed and which may remain. APT threats abuse many of these areas to avoid inspection.

By the end of this session will also show you how to walk a page table, why Windows8 makes life easier, what to look for and how to obtain a comprehensive understanding of what possible code is hiding/running on your computer.

Final thoughts on using a VM memory snapshot to fully describe/understand any possible code running on a Windows system.

Catching Malware En Masse: DNS and IP Style

Dhia Mahjoub, Senior Security Researcher, OpenDNS
Thibault Reuille, Security Researcher, OpenDNS Inc
Andree Toonk, Manager of Network Engineering, OpenDNS
12:00 in Track Three

The Internet is constantly growing, providing a myriad of new services both legitimate and malicious. Criminals take advantage of the scalable, distributed, and rather easily accessible naming, hosting and routing infrastructures of the Internet. As a result, the battle against malware is raging on multiple fronts: the endpoint, the network perimeter, and the application layer. The need for innovative measures to gain ground against the enemy has never been greater.

In this talk, we will present a novel and effective multi-pronged strategy to catch malware at the DNS and IP level, as well as our unique 3D visualization engine.

We will describe the detection systems we built, and share several successful war stories about hunting down malware domains and associated rogue IP space.

At the DNS level, we will describe original methods for tracking botnets, both fast flux and DGA-based. We use a combination of fast, light-weight graph clustering and DNS traffic analysis techniques and threat intelligence feeds to rapidly detect botnet domain families, identify new live CnC domains and IPs, and mitigate them.

At the IP level, classical reputation methods assign "maliciousness" scores to IPs, BGP prefixes, or ASNs by merely counting domains and IPs. Our system takes an unconventional approach that combines two opposite, yet complementary views and leads to more effective predictive detections.

(1) On one hand, we abstract away from the ASN view. We build the AS graph and investigate its topology to uncover hotspots of malicious or suspicious activities and then scan our DNS database for new domains hosted on these malicious IP ranges. To confirm certain common patterns in the AS graph and isolate suspicious address space, we will demonstrate novel forensics and investigative methods based on the monitoring of BGP prefix announcements.

(2) On the other hand, we drill down to a granularity finer than the BGP prefix. For this, we zero in on re-assigned IP ranges reserved by bad customers within large prefixes to host Exploit kit domains, browlock, and other attack types. We will present various techniques we devised to efficiently discover suspicious smaller ranges and sweep en masse for candidate suspicious IPs.

Our system provides actionable intelligence and preemptively detects and blocks malicious IP infrastructures prior to, or immediately after some of them are used to wage malware campaigns, therefore decisively closing the detection gap. During this presentation, we will publicly share some of the tools we built to gather this predictive intelligence.

The discussion of these detection engines and "war stories" wouldn't be complete without a visualization engine that adequately displays the use cases and offers a graph navigation and investigation tool.

Therefore, in this presentation, we will present and publicly release for the first time our own 3D visualization engine, demonstrating the full process which transforms raw data into stunning 3D visuals. We will also present different techniques used to build and render large graph datasets: Force Directed algorithms accelerated on the GPU using OpenCL, 3D rendering and navigation using OpenGL ES, and GLSL Shaders. Finally, we will present a few scripts and methods used to explore our large networks. Every concept is intended to detect and highlight precise features and will be presented with its corresponding visual representation related to malware detection use cases.

Open Source Fairy Dust

John Menerick, Security Researcher, Netsuite
12:00 in Track Two

Over the past 30 years, the Internet and open source software have worked in tandem. The Internet has provided an environment for open source software to prosper. Some would say the Internet and open source software are indistinguishable. From low level cryptography to critical services, the Internet's foundation is built upon open source building blocks. These blocks are crumbling.

This presentation will tread through popular open source projects, common fallacies, peer into 0days, walk trends, and break code. When we are finished, you will be able to use the same techniques and tools to break or protect the Internet's building blocks.

Generating ROP payloads from numbers

Alexandre Moneger, Cisco Systems
14:00 in Track Three

Is it possible to generate a ROP payload whilst using as few gadgets from the target binary as possible? Is it also possible to build any shellcode in memory regardless of the opcodes in the target binary? An approach to this is to build the ROP payload by summing selected pieces of memory together and copying them to a stack in the process address space. A method and tool will be presented, which allows to stitch together selected numbers found in memory into a payload and execute it.

Return Oriented Programming is at the core of modern exploitation technics, but the automation of the payload generation can be time consuming. The intent was to write a tool which is able to generate a generic enough ROP payload that it worked in most situations. I will present a new method to generate ROP payloads which relies on very few gadgets within the target binary (sometimes none), nor will rely on string copying particular bytes to build the in memory payload.

NSA Playset : GSM Sniffing

Pierce, Security Researcher
Loki, Security Researcher
12:00 in Track One

A5/1, as implemented in GSM, was broken wide open in 2003, yet GSM is still the most widely used mobile communications protocol in the world. Introducing TWILIGHTVEGETABLE, our attempt to pull together the past decade of GSM attacks into a single, coherent toolset, and finally make real, practical, GSM sniffing to the masses.

You're Leaking Trade Secrets

Michael Schrenk, Business Intelligence Specialist
11:00 in DEF CON 101 Track

Networks don't need to be hacked for information to be compromised. This is particularly true for organizations that are trying to keep trade secrets. While we hear a lot about personal privacy, little is said in regard to organizational privacy. Organizations, in fact, leak information at a much greater rate than individuals, and usually do so with little fanfare. There are greater consequences for organizations when information is leaked because the secrets often fall into the hands of competitors. This talk uses a variety of real world examples to show how trade secrets are leaked online, and how organizational privacy is compromised by seemingly innocent use of The Internet.

Android Hacker Protection Level 0

Tim Strazzere, Lead Research & Response Engineer
Jon Sawyer, CTO of Applied Cybersecurity LLC
14:00 in DEF CON 101 Track

Obfuscator here, packer there - the Android ecosystem is becoming a bit cramped with different protectors for developers to choose. With such limited resources online about attacking these protectors, what is a new reverse engineer to do? Have no fear, after drinking all the cheap wine two Android hackers have attacked all the protectors currently available for everyones enjoyment! Whether you've never reversed Android before or are a hardened veteran there will be something for you, along with all the glorious PoC tools and plugins for your little heart could ever desire.

sunday presentations

"Around the world in 80 cons" – A Perspective

Jayson E. Street, Senior Partner of Krypton Security

10:00 in DEF CON 101 Track

After spending 15 years in the hacker / InfoSec community, I thought it was time to pause and look back upon all I have seen, everywhere I have been, all the people I met and everything I have learned. And then share some of that knowledge with people to hopefully help them have a leg up moving forward. More importantly, compare and contrast my experiences and perspectives with statistics we commonly see based on attacks and the countries of origin. Statistics tell one story, perspective tells the other. This is a talk on perspectives.

Hackers, and hacking, are perceived differently around the world and, in turn, some view our community and what we do with different eyes than ours. I believe most reports/papers we (Americans) see about that topic are skewed and never give an accurate global image. Taking a very small dose of reality and comparing it to what we're subjected to, is interesting. Being a foreign hacker attending a con, or delivering an engagement, in an alien land often led to unexpected situations that I will also share.

I will also share while searching for diversity in our global hacking culture I found things that united us more than you would expect. I show how no matter what region of the planet you come from we face a threat we all need to face and overcome.

Playing with Car Firmware or How to Brick your Car

Paul Such 0x222, Founder of SCRT Agix, SCRT

13:30 in Track One

A lot of papers have already been done/ produced on hacking cars through ODB2/ CanBus. Looking at the car firmware could also be something really fun :) How to access the firmware, hidden menus & functionalities, hardcoded SSID, users and passwords (yes, you read right), are some of the subjects we will cover during this short presentation.

Optical Surgery; Implanting a DropCam

Patrick Wardle, Director of Research, Synack

Colby Moore, Security Research Engineer, Synack

11:00 in Track Two

Video Monitoring solutions such as DropCam aim to provide remote monitoring, protection and security. But what if they could be maliciously subverted? This presentation details a reverse-engineering effort that resulted in the full compromise of a DropCam. Specifically, given physical access and some creative hardware and software hacks, any malicious software may be persistently installed upon the device.

Implanting a wireless video monitoring solution presents some unique opportunities, such as intercepting the video stream, 'hot-micing', or even acting as persistent access/attack point within a network. This presentation will describe such an implant and well as revealing a method of infecting either Windows or OS X hosts that are used to configure a subverted DropCam.

New Village proposals

There are a couple of proposals for new DEF CON villages in the mix, and we invite you to join in the discussion if one of them interests you! Check out the proposals below and get your self involved in the next DEF CON village!

Prepper Village:
Are you ready for the inevitable zombie apocalypse? Got survival skills? Come share your ideas for a possible Prepper Village at DEF CON 23, Friday at 15:00 in the Belize meeting room!

Bio Hacking Village :
Greetings, fellow earthlings! Are you interested in hacking biology to be more useful or secure. We are! How about cybernetics, bio-nanotechnology, and potential immortality? Who isn't? Perhaps you should attend the DEF CON Bio Hacker Village proposal/planning meeting on Saturday at noon in the Belize conference room. All are welcome as long as the ideas, proposals, and content are constructive and responsible. We should learn to hack biology now, as it will inevitably hack us. Please check out defconbiohackingvillage.org to learn more & please feel free to get involved! We hope to launch next year. -DC_BHV Proposal Team

DEF CON GROUPS

Every month, all around the globe, hackers and similar minded professionals meet up to learn and share new ideas. In coffee shops, libraries, homes, and bars around the globe - the world's DEF CON groups extend DEF CON year round. The DCG program is designed to help people learn new things and ensure cohesion in the hacker community as a whole. We have more than 300 groups that are active in over 20 countries, and are expanding our reach every year!

This year was the first annual DCG Challenge! Participating groups were sent 20 Parallax boards [DEF CON 20 Badges] and a mission:

To build a DC20 badge network, cluster, or mesh, capable of performing a unified task, that

the group defines.

How many badges they decide to use, the purpose of the work they perform, and how they communicate, was up to each DEF CON Group. This year we had 6 participating groups.

I am proud to annouce that DC530 are the first place winners of the first DCG Challenge! That's 8 human badges heading their way! Good job, DC530.

Check the DC Community area on defcon.org for more information regarding the groups, group listings, and signup information. The DEF CON forums is also a great place to receive announcements. As always, you can hit us on twitter [@defcongroups] .

Have a great DC22 - and happy hacking!

shoutz out to Salem, a pok, s0ups, and blakBunny for all their work on the backend work year round that keeps the DCG program running! A very big thankyou!

-blakdayz [blak@defcon.org]

DC530

Hey you! Yeah you!!!! Do you like laser tag? Do you want to play laser tag at DEF CON? If you answered yes, YOU'RE IN LUCK! The DC530 crew has designed and built a laser tag game out of DEF CON 20 badges and brought it to Vegas for everyone to play. Head over to the Scavenger Hunt table to check it out. If you've got a DC20 badge, get our code flashed onto your badge and pick up a small parts kit to build a fully functional laser blaster.

shout outs to the project participants: Sarif, Ychto, Tim, Sam, Cereal, Salem, Wolf.

-DC530

Movie Night with the Dark Tangent

Special guests: Director Brian Knappenberger and Noah Swartz, Aaron's brother. Q&A to follow screening.

'The Internet's Own' boy tells the story of Aaron Swartz. Aaron helped create the bedrock RSS protocol, helped found the Internet hive mind Reddit and evangelized for real openness in our shared digital space. At the age of 26, facing hyper-agressive prosecution for Computer Fraud and Abuse Act violations, he took his own life. The story of that life, and the powerful forces that combined to silence it, will humble, amaze and enrage you. It should also make you more committed to building the Internet we want.

Friday at 21:00 in Track 3

Special guest: Director Will Eubank.

'The Signal' is an ambitious and inventive sci-fi thriller that takes place on a road trip to DEF CON. Satisfyingly cerebral and viscerally gripping, it goes none of the places you most expect. The less you know going in, the better, but be prepared for a rare treat: a summer sci-fi film that respects its audience and delivers the mindbending plot twists and staggering visuals that make the genre great.

Saturday at 21:00 in Track 3

DEF CON Social

@_defcon_

facebook.com/defcon

youtube.com/user/DEFCONConference

google.com/+DefconOrgplus

defcon.org/defconrss.xml

DEF CON is never not happening. Well, for a week or so after the event in Vegas it's kind of not happening. For that week, DEF CON is getting spa treatments and taking power naps. Otherwise, however, DEF CON is always going on. DEF CON groups are meeting, DEF CON plans are being made in the Forums and we're sharing with everyone on social media. If you're already connecting with us, thank you. If you aren't, please do. Join a DC Group, register for the Forums, follow us on Facebox and Tweeter. DEF CON community is always happening, and there's always room for you.

Hacker Jeopardy

RATED PG

FOR KIDS

GOOGLE THIS!
PORT MATH
ACRONYMS
INTERNET HISTORY
HTML
FAMOUS HACKERS
MOVIE HACKS
PASSWORDS
AND MORE!

6 Teams of 3 members will compete for prizes & bragging rights at DefCon Kids.

Everyone is invited!

Don't Miss the Fun with your hosts: Winn, Miss Kitty and Miss Tiffany!

Sunday 1pm *SHARP* · Crown Theatre
Game 1: 7-12 yrs old · Game 2: 13-17 yrs old

DEF CON VENDORS

purveyors of fine hacker-related merchandise

ACLU

The American Civil Liberties Union is one of the nation's oldest and largest legal and advocacy organizations. With affiliates in all 50 states, we work daily in the courts, Congress, state legislatures, and communities to defend the individual rights and liberties protected by the Constitution.

The ACLU's Speech, Privacy, and Technology Project and National Security Project seek to ensure that civil liberties are enhanced rather than compromised by new advances in science and technology. We work to rein in the government's unfettered surveillance of your communications, to challenge the ability of corporations to profit from your data without appropriate privacy protections, and to limit law enforcement's warrantless access to your private information. And we'll keep fighting, because you shouldn't have to give up on your rights to use the technology of modern life.

BREAKPOINT BOOKS

BreakPoint Books is your official conference bookstore on site at DEF CON. We'll have all your favorite books for sale and we're conveniently located in the Vendor Area. Make sure to stop by and view the titles in stock and purchase a few written by some of your favorite authors!

BUMP MY LOCK

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 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!

CAPITOL COLLEGE

Founded in 1927, Capitol College is the only independent school in Maryland dedicated exclusively to Cybersecurity, Engineering, Computer Sciences and Management. Designated as a "Center of Academic Excellence", Capitol offers a fully accredited set of undergraduate and graduate degree programs, including our Doctorate of Sciences in Information Assurance. Delivered "live" online, our graduate courses will fit most any schedule, pace or budget! So whether you're a Neo or a Ninja, Capitol has the key to your advancement! Admissions representatives, faculty, current students and alumni will be at our booth in the exhibit hall to share information and opportunities!

CARNEGIE MELLON UNIVERSITY

The Information Networking Institute (INI) offers full-time master's degrees in information security at Carnegie Mellon University, the home and hotbed of smart students who desire to make an impact, whether it be starting the campus grappling club or dominating in Capture the Flag. The INI offers interdisciplinary programs with curricula that span several top-ranking colleges. As a result, the graduates of the INI move on to apply their know-how at some of the most competitive places, like Silicon Valley, Wall Street, and the DoD, as well as their own startups. Full scholarships are available for U.S. citizens. Talk with Kari for details.

COBALT STRIKE

Cobalt Strike is threat emulation software. Execute targeted attacks and evade defenses in a way that replicates a well-funded actor with custom tools. Key features include robust communication over DNS and SMB pipes, man-in-the-browser session hijacking, and flexible beaconing to multiple hosts. This is NOT compliance testing.

EFF

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy and free expression online through a strategic combination of impact litigation, policy analysis, education, and grassroots activism. We empower tinkerers, creators, coders, and consumers to reclaim freedom as our use of technology grows.

GHETTOGEEKS

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).

GHOSTERY

Ghostery is a global marketing technology company that provides online transparency and control to individuals. Millions of people around the world have installed Ghostery's easy to use browser plug-in to see and manage the information they share with companies online.

GUNNAR

GUNNAR is the only patented computer eyewear recommended by doctors to protect and enhance your vision. GUNNARS alleviate all common causes of digital eye strain and visual fatigue. The result - improved clarity, focus and performance for anyone using a computer for working, hacking or coding the next big thing.

THE HACKER ACADEMY

The Hacker Academy is trusted by some of the world's largest and most notable organizations to educate and secure their staff; both technical and non-technical alike. THA provides members with an engaging, cloud based, security training environment so that they can learn the latest information security techniques and push their technical limits at their own pace. With lessons in courses including Ethical Hacking, Penetration Testing, Reverse Engineering, and Digital Forensics, there's something for everyone. Our Role Based, Security Awareness training program is specifically designed for each and every employee within an organization. Our philosophy is to arm all of our members with the knowledge necessary to practice, implement, and deploy what they have learned immediately and effectively.

HACKERS FOR CHARITY

Hackers for Charity is a non-profit organization that leverages the skills of technologists. We solve technology challenges for various non-profits and provide food, equipment, job training and computer education to the world's poorest citizens.

HACKERSTICKERS.COM

Get ready for DEF CON and grab a fresh t-shirt over at HackerStickers.com or order a replacement for that special con shirt that got destroyed from years of use and abuse! HackerStickers has all your lock picking gear and a lock pick board on site for you to learn and practice on! Sign up for the HackerStickers newsletter for a sneak peak on the latest designs and to get a free sticker!

HACKER WAREHOUSE

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we strive to 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

HakShop: host of security products from world renowned researchers, is your source for the highest quality hacker gadgets. With an arsenal of WiFi honey-pots, HID attack tools, Wireless brute-forcers and even monitoring equipment — let's just say if 007 were a pen-tester he'd be rocking our gear. Come by our booth today for a demo by Shannon Morse of Hak5

IFORCE

Mr. Michael Miklich is President and Founder of Institute for Cybersecurity Education, whose mission is to develop, promote, implement, support, teach and track cybersecurity education at the secondary school level.

ITUS NETWORKS

tus Networks brings families best-in-class threat prevention for their home Internet connection at affordable prices. Our network security systems are specially designed to block cyber attacks while filtering out malware and other undesirable content with zero configuration or technical knowledge required. At Itus Networks, we believe all families deserve peace of mind that the devices connected to their home network are secure and protected 24-hours a day, 7 days a week.

LBGFX

Customize T shirts & Stickers on the spot at DEF CON 22!

NO STARCH PRESS

No Starch Press publishes books for geeks and hackers of all ages. Our titles have personality, our authors are passionate, and we read and edit every book that we publish.

We'll be hosting book signings at our community table in the DEF CON Vendor Area. Visit nostarch.com/defcon for a full signing schedule. All No Starch Press books will be discounted 30% and come with a DRM-free ebook.

NUAND

Nuand provides low-cost, USB 3.0 SDRs (Software Defined Radio) for enthusiasts, and experts a like. After a successful Kickstarter, bladeRF is now available and ready for use in your projects! Stop by our table to see our demos and find out more about bladeRF, GNURadio, OpenBTS and Software Defined Radios!

PENTESTER ACADEMY

80+ hrs Comprehensive, Hands-on, Highly Technical training trusted by professionals from 75+ Countries

PRIVACY CASE

The Privacy Case uses military-grade shielding technology to give you the ability to block unwanted intrusions into your cell phones and wireless devices. By controlling when and where your phone can send and receive information, the PrivacyCase prevents remote activation, GPS location-tracking and real-time audio/video eavesdropping.

PWNIE EXPRESS

Pwnie Express is the leading provider of network security assessment solutions for remote locations and wireless. Thousands of enterprises and government organizations worldwide rely on Pwnie Express's products for asset discovery, vulnerability assessment, and drop-box penetration testing and obtain unprecedented insight into their distributed network infrastructure. Pwnie Express smart devices leverage open source tools.

DEF CON VENDORS

RAPID7

Rapid7 security software helps organizations reduce threat exposure and detect compromise. Metasploit, founded by HD Moore and acquired by Rapid7 in 2009, remains the world's most popular open source penetration testing tool with a 200,000 member strong community. The Rapid7 table will be selling special edition Metasploit t-shirts with all proceeds going to the EFF.

SECURENINJA

While SecureNinja generally provides Cybersecurity Training and Consulting Services across the globe, every year at DEF CON we get a little crazy and bring out our amazing line of ninja gear.

Whether you're a SecureNinja Cybersecurity Alumni, a future hacker, or a ninja in training, we'll have something for you AND your friends at home. Come by our table to check out and deck out in our ninja gear for men, women, teens, kids and even baby ninjas. That's right, baby ninjas.

Want a taste of what may be in store? Check out our Instagram or Twitter for ninja gear photos @secureninja.

SECURITY SNOBS

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, TiGr, and Sargent and Greenleaf. Visit https://SecuritySnobs.com for our complete range of products. Stop by our booth and get free shipping on items for the month following the conference. Featuring the mobile alarm system, unique cutaways, $1500+ padlocks, and a variety of other unique products.

SEREPICK

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. The Full product range of SPARROWS lock picks and tools will also be available including their newly released COFFIN KEYS, Safe Cracker and EOD set. All products will be demonstrated at various times and can be personally tested for use and Efficacy.

SIMPLE WIFI

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.

SVX

Hacker-relevant-artistically-driven-limited-production DJ Mixes, Clothing, Stickers, Posters, Buttons, and more... Listen for the music!

TOOOL

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 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 locksport and hacker community.

UNIVERSITY OF ADVANCING TECHNOLOGY

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.

UNIXSURPLUS

"Home of the $99 1U Server"

1260 La Avenida St Mountain View, CA 94043

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

SHORT STORY CONTEST

The theme for the DEF CON 22 Short Story Contest was 'The Future is Now'. We asked you to take a long look into the technological side of the near future and bring it back to us, in the form of a short story with some connection to DEF CON. We thank everybody who took the time to share their work with us, and we've included every single entry on the conference CD you likely picked up with this program. If somehow you have this program but no conference CD, you can read all the submissions on forum.defcon.org. Also, HOW DID YOU GET THIS PROGRAM? ARE YOU FROM THE FUTURE?

We're always blown away by the creativity of the DEF CON community. We hope to see more of you competing in this contest next year. And by hope we mean expect. And by next year we mean you can start writing now. We don't have the theme yet, but it's gonna be DEF CON related and science-fictiony so get on it.

2014 Winners

First Place – Two Human Badges
Title: "Hide it Well" Authors: Todd Carr (@frozenfoxx) and Leah Figueroa(@sweet_grrl)

Second Place – One Human Badge
Title: "We are Not Just Bodies" Author: Jacie Jones

People's Choice Award – One Human Badge
Title: "A Dispatch from DEF CON" Author: Rob Pait

ART CONTEST

Congratulations to the winners of the 2014 DEF CON Art Contest!

First Place and People's Choice

Alice in Hackerland by Tess Schrodinger

Second Place

Helicopter Parents Weren't This Bad by Amit Yehuda

Third Place

Bleed by Joey Strine

Thanks to everyone who submitted work. There is no end to the hidden talents of the DEF CON massive. You can take a look at all the entries on our Facebook page. Also, don't let the contest ending stop you - if you have the urge to create some on-theme artworks between now and the DEF CON 23, we'd be happy to share them with the world. You might not win anything beyond our love and gratitude, but that's not exactly nothing.

BOOK SIGNINGS

Technical conferences like DEF CON are crawling with authors. The good kind – the ones who write thick, practical books about very specific topics. For your convenience, we're keeping a bunch of exactly this type of writer at the Breakpoint table. Please stop by, paw the merchandise and maybe even get a book or two signed. If you still do your technical reading in meatspace, that is.

	Friday	Saturday	Sunday
11:00	"Hacking Point of Sale: Payment Application" by Slava Gomzin	"Mind Games" by Richard Thieme	
12:00	"Android Hacker's Handbook" by Joshua Drake, Charlie Miller, Zach Lanier	"Penetration Testing: A Hands On Introduction to Hacking" by Georgia Weidman	"Webbots, Spiders and Screen Scrapers, 2nd Ed." byMike Schrenk
13:00	"The Browser Hacker's Handbook " by Wade Alcorn and Michele Orru	"Threat Modeling: Designing for Security" by Adam Shostack	"Social Engineering: The Art of Human Hacking", "Unmasking the Social Engineer: The Human Element of Security" by Chris Hadnagy
14:00	"The Art of Intrusion", "The Art of Deception", "Ghost in the Wire" by Kevin Mitnick	"The IDA Pro Book" by Chris Eagle	
16:00	"Metasploit: The Penetration Tester's Guide" by Jim Gorman, Devon Kearns, Dave Kennedy, Mati Aharoni		

THURSDAY August 7th

	Track 3	DEF CON 101
10:00	**DEF CON 101 - The Talk** Panel	**Data Protection 101 - Successes, Fails, and Fixes** PTzero (Peter Teoh)
11:00		**Practical Foxhunting 101** SimonJ
12:00	**Paging SDR... Why should the NSA have all the fun?** Xaphan & Noobz	**RF Penetration Testing, Your Air Stinks** RMellendick & DaKahuna
13:00	**Protecting SCADA From the Ground Up** AlxRogan	**AWS for Hackers** Beaker
14:00	**One Man Shop: Building an Effective Security Program All By Yourself** Medic	**Anatomy of a Pentest; Poppin' Boxes like a Pro** Pushpin
15:00	**In the forest of knowledge with 1o57** LosT	**Standing Up an Effective Penetration Testing Team** Wiseacre
16:00	**Oh Bother, Cruising the Internet With Your Honeys – Creating Honeynets for Tracking Criminal Organizations** Terrence Gareau & Mike Thompson	**The Making of DEF COIN** Xaphan, Beaker, & Anch
17:00	**RFIDler: SDR.RFID.FTW** Major Malfunction and Zac Franken	**Reverse Engineering Mac Malware** Sarah Edwards

Friday August 8th

	Penn & Teller	Track 1	Track 2	Track 3	DEF CON 101
10:00	**Welcome & Making of the DEF CON Badge** Dark Tangent & LosT	**Saving the Internet (for the Future)** Jay Healey	**Domain Name Problems and Solutions** Paul Vixie	**Oracle Data Redaction is Broken** David Litchfield	**Meddle: Framework for piggy-back fuzzing and tool development** Geoff McDonald
11:00	**Steganography in Commonly Used HF Radio Protocols** Paul Drapeau & Brent Dukes	**The Only Way to Tell the Truth is in Fiction: The Dynamics of Life in the National Security State** Richard Thieme	**Measuring the IQ of your Threat Intelligence feeds** Alex Pinto & Kyle Maxwell	**Abuse of Blind Automation in Security Tools** Eric (XlogicX) Davisson & Ruben Alejandro (chap0)	**USB for all!** Jesse Michael & Mickey Shkatov
12:00	**The NSA Playset: RF Retroxeflectors** Michael Ossmann	**How To Get Phone Companies To Just Say No To Wiretapping** Phil Zimmermann	**Stolen Data Markets An Economic and Organizational Assessment** Dr. Thomas Holt, Olga Smirnova, & Yi-Ting Chua	**From root to SPECIAL: Pwning IBM Mainframes** Philip "Soldier of Fortran" Young **The $env:PATH less Traveled is Full of Easy Privilege Escalation Vulns** Christopher Campbell	**We Wrapped Samba So You Don't Have To** Lucas Morris & Michael McAtees
13:00	**Hacking US (and UK, Australia, France, etc.) traffic control systems** Cesar Cerrudo	**Detecting and Defending Against a Surveillance State** Robert Rowley	**PoS Attacking the Traveling Salesman** Alex Zacharis & Tsagkarakis Nikolaos	**Bypass firewalls, application white lists, secure remote desktops under 20 seconds** Zoltán Balázs	**Investigating PowerShell Attacks** Ryan Kazanciyan & Matt Hastings
14:00	**What the Watchers See: Eavesdropping on Municipal Mesh Cameras for Giggles (or Pure Evil)** Dustin Hoffman & Thomas (TK) Kinsey	**Hacking the FBI: How & Why to Liberate Government Records** Ryan Noah Shapiro	**DEF CON Comedy Jam Part VII, Is This The One With The Whales?** Panel	**Extreme Privilege Escalation On Windows 8/ UEFI System** Corey Kallenberg & Xeno Kovah	**Client-Side HTTP Cookie Security: Attack and Defense** David Wyde
15:00	**Am I Being Spied On? Low-tech Ways Of Detecting High-tech Surveillance** Dr. Phil Polstra	**Saving Cyberspace by Reinventing File Sharing** Eijah		**Veil-Pillage: Post-exploitation 2.0** Will Schroeder (@harmj0y)	**An Introduction to Back Dooring Operating Systems for Fun and Trolling** Nemus
16:00	**Practical Aerial Hacking & Surveillance** Glenn Wilkinson	**The Open Crypto Audit Project** Kenneth White & Matthew Green	**Ephemeral Communications: Why and How?** Panel	**Acquire current user hashes without admin privileges** Anton Sapozhnikov	**Blinding The Surveillance State** Christopher Soghoian
17:00		**Dark Mail** Ladar Levison & Stephen Watt	**From Raxacorico-fallapatorius With Love: Case Studies In Insider Threat** Tess Schrodinger	**Why Don't You Just Tell Me Where The ROP Isn't Suppose To Go?** David Dorsey **The Secret Life of Krbtgt** Christopher Campbell	**Diversity in Information Security** Panel
18:00			**A journey to protect points-of-sale** Nir Valtman		

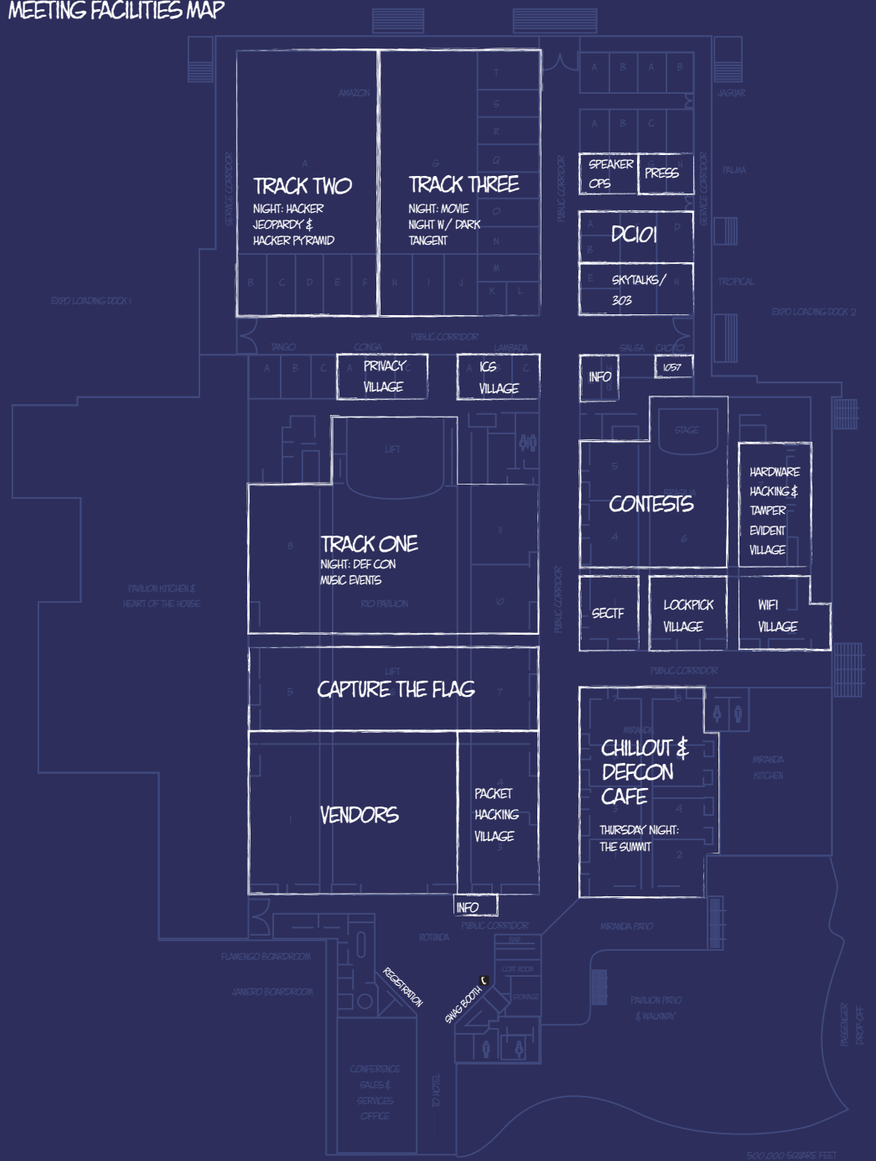
saturday August 9th

	Penn & Teller	Track 1	Track 2	Track 3	DEF CON 101
10:00	**The Cavalry Year[0] & a Path Forward for Public Safety** Joshua Corman & Nicholas J Percoco	**Hack All The Things: 20 Devices in 45 Minutes** CJ Heres, Amir Etemadieh, Mike Baker, & Hans Nielsen	**Hacking 911: Adventures in Disruption, Destruction, and Death** Christian "quaddi" Dameff, Jeff "r3plicant" Tully & Peter Hefley	**Mass Scanning the Internet: Tips, Tricks, Results** Robert Graham, Paul McMillan, & Dan Tentler	**Screw Becoming A PentesterWhen I Grow Up I Want To Be A Bug Bounty Hunter!** Jake Kouns & Carsten Eiram
11:00	**Don't Fuck it Up!** Zoz	**The Internet of Fails: Where IoT Has Gone Wrong and How We're Making It Right** Mark Stanislav & Zach Lanier	**Girl… Fault-Interrupted.** Maggie Jauregui	**I Hunt TR-069 Admins: Pwning ISPs Like a Boss** Shahar Tal	**Bug Bounty Programs Evolution** Nir Valtman
12:00	**Summary of Attacks Against BIOS and Secure Boot** Yuriy Bulygin, Oleksandr Bazhaniuk , Andrew Furtak & John Loucaides	**Home Insecurity: No alarms, False alarms, and SIGINT** Logan Lamb	**Cyberhijacking Airplanes: Truth or Fiction?** Dr. Phil Polstra & Captain Polly	**Don't DDoS Me Bro: Practical DDoS Defense** Blake Self & Shawn "cisc0ninja" Burrell	**How to Disclose an Exploit Without Getting in Trouble** Jim Denaro & Tod Beardsley
13:00	**Secure Random by Default** Dan Kaminsky	**PropLANE: Kind of keeping the NSA from watching you pee** Rob Bathurst, Russ Rogers, Mark Carey, & Ryan Clarke	**Just What The Doctor Ordered?** Scott Erven & Shawn Merdinger	**Secure Because Math: A Deep Dive On Machine Learning-Based Monitoring** Alex Pinto	**Instrumenting Point-of-Sale Malware: A Case Study in Communicating Malware Analysis More Effectively** Wesley McGrew
14:00		**NinjaTV - Increasing Your Smart TV's IQ Without Bricking It** Felix Leder		**Masquerade: How a Helpful Man-in-the-Middle Can Help You Evade Monitoring** Ryan Lackey, Marc Rogers, & theGrugq	**The Monkey in the Middle: A pentesters guide to playing in traffic.** Anch (MIKE GUTHRIE)
15:00	**Advanced Red Teaming: All Your Badges Are Belong To Us** Eric Smith & Josh Perrymon	**A Survey of Remote Automotive Attack Surfaces** Charlie Miller & Chris Valasek	**Impostor – Polluting Tor Metadata** Charlie Vedaa & Mike Larsen **Check Your Fingerprints: Cloning the Strong Set** Richard Klafter (Free) & Eric Swanson (Lachesis)	**VoIP Wars: Attack of the Cisco Phones** Fatih Ozavci	**Detecting Bluetooth Surveillance Systems** Grant Bugher
16:00	**Manna from Heaven: Improving the state of wireless rogue AP attacks** Dominic White & Ian de Villiers	**Learn how to control every room at a luxury hotel remotely** Jesus Molina **Raspberry MoCA - A recipe for compromise** Andrew Hunt	**Panel: Ask the EFF: The Year in Digital Civil Liberties** Kurt Opsahl, Nate Cardozo, Mark Jaycox, Yan Zhu, & Eva Galperin	**Abusing Software Defined Networks** Gregory Pickett	**Touring the Darkside of the Internet. An Introduction to Tor, Darknets, and Bitcoin** Metacortex & Grifter
17:00		**Attacking the Internet of Things using Time** Paul McMillan		**Getting Windows to Play with Itself: A Hacker's Guide to Windows API Abuse** Brady Bloxham	**DEF CON the Mystery, Myth and Legend?**
18:00			**Old Skewl Hacking: Porn Free!** Major Malfunction	**Panel – Surveillance on the Silver Screen- Fact or Fiction?** Nicole Ozer, Kevin Bankston, & Timothy Edgar	

sunday August 10th

	Track 1	Track 2	Track 3	DEF CON 101
10:00	**Burner Phone DDOS 2 dollars a day : 70 Calls a Minute** Weston Hecker	**Weaponizing Your Pets: The War Kitteh and the Denial of Service Dog** Gene Bransfield	**I am a legend: Hacking Hearthstone with machine learning** Elie Bursztein & Celine Bursztein	**"Around the world in 80 cons" - A Perspective** Jayson E. Street
11:00	**NSA Playset: DIY WAGONBED Hardware Implant over I2C** Josh Datko & Terry Reed	**Optical Surgery; Implanting a DropCam** Patrick Wardle & Colby Moore	**The Simple Route to Backbone Routers** Luca "kaeso" Bruno & Mariano "emdel" Graziano	**You're Leaking Trade Secrets Michael** Schrenk
12:00	**NSA Playset : GSM Sniffing** Pierce & Loki	**Open Source Fairy Dust John** Menerick	**Catching Malware En Masse: DNS and IP Style** Dhia Mahjoub, Thibault Reuille, & Andree Toonk	**Dropping Docs on Darknets: How People Got Caught** Adrian Crenshaw
13:00	**Blowing up the Celly - Building Your Own SMS/MMS Fuzzer** Brian Gorenc & Matt Molinyawe **Playing with Car Firmware or How to Brick your Car** Paul Such 0x222 & Agix	**Deconstructing the Circuit Board Sandwich: Effective Techniques for PCB Reverse Engineering** Joe "Kingpin" Grand	**Weird-Machine Motivated Practical Page Table Shellcode & Finding Out What's Running on Your System** Shane Macaulay	**Home Alone with localhost: Automating Home Defense** Chris Littlebury
14:00	**Empowering Hackers to Create a Positive Impact** Keren "k3r3n3" Elazari	**NSA Playset: PCIe Joe FitzPatrick &** Miles Crabill	**Generating ROP payloads from numbers** Alexandre Moneger	**Android Hacker Protection Level 0** Tim Strazzere & Jon Sawyer
15:00	**Elevator Hacking - From the Pit to the Penthouse** Deviant Ollam & Howard Payne	**Contests Awards Ceremony**	**Shellcodes for ARM: Your Pills Don't Work on Me, x86** Svetlana Gaivoronski & Ivan Petrov	**Is This Your Pipe? Hijacking the Build Pipeline** Kyle Kelley & Greg Anderson
16:30		**DEF CON 22 Closing Ceremony**		

RIO ALL-SUITE HOTEL & CASINO
MEETING FACILITIES MAP



thank you!

Putting together a conference takes a lot of people, a lot of energy and creativity, as well as sacrifice of time and money. Many contest and village organizers put in all of that and more year round to make DEF CON a success. I want to thank them all. I want to also thank all the CON volunteers who work in front, and behind, the curtain to make everything happen. The stories we could tell! I sometimes think of my role as that of a conductor. No music is made without a symphony to back you up, and everyone on this page (+more) are part of that symphony! I want to call out a special thanks to those Goons who keep coming back for more punishment, you'll see some with patches commemorating the number of years they have served the community, with 2, 5, 10, and 15 year editions newly made this year. I am very proud of what we managed to pull off this year. Next year promises to be a whole new adventure. -The Dark Tangent

Lockheed wants to thank Will for doing an extraordinary job making things run smoothly for con-operations. Also thank you to every department head for pulling together as a team and making this look "easy"! Thanks to all the Goons for all their tireless, thankless hours of volunteer effort towards this herculean effort. And thank you to the attendees - without you we wouldn't even do this - I hope this is the best con yet for you!

1o57 would like to thank DT, Neil & Kita, eChan (you're the best), Clutch and Zant, Russman, KenG and JonMac, and all the crew in the APG, and everyone who participates in the challenges each year. Duo xie.

Press would like to thank Nic0, Dirk, DeadAddict, Nikki, Heathers, Rich, Jim, Jerry, Alex, Authur, noise, Melanie, and sleestak.

Heather would like to thank the Comms/Dispatch Staff: Ahab, RF, Asmodian, Voltage Spike, Nulltone, Bonita, Counterglitch, and Fosgood for supporting DEF CON.

Krassi would like to thank Jeremy for supporting the con!

Pyr0 and the Contest team would like to thank to following: hackajar, c013slaw, tener, panadero, 0x58, sidragon, mohgarr, phorkus, EvilRob, phartacus, shaggy, cyungle, turb1n3, kos, knight owl, bo knows, zoz, clutch, y3t1, bombNav, afterburn, kingpin, stealth, C.Ingram, timelord, 0ccupant, RussR, Dark Tangent, Nikita, Neil, Will, and Charel for their tireless support of the Contests, Villages and Events at DEF CON. In addition, all the groups that host all the wonderful Contests, Villages and Events... You make life worth living!

Cjunky would like to thank Alex C, Amber, Angie, Arclight, Bruce, B0n3z, BeaMeR, Blakdayz, Captain, Carric, CHRIS, cRusad3r, Cyber, Cymike, Dallas, Dc0de, Deelo, Dr3t, Eddy Current, EmergencyMexican, Evil, Flea, FoxCaptain, Freshman, Gadsden, Gonzo, Godminusone, HattoriHanzo, HausCat, Iole, JAFO, Jake, John Doll, JustaBill, Kallahar, KevinE, Knox, Kruger, Lei, Lordy, Mattrix, Montell, MrB0t, Noid, Nynex, P33v3, Pappy, Pfriedma, Phreck, Plasma, Polish Dave, Priest, Quiet, Rik, Salem, Siviak, SkyDog, Stan, Synn, Tacitus, Thomas, Trinity, Vidiot, Viss, Wham, WhiteB0rd and our many volunteers. PAX PER IMPERIUM.

ChrisAM would like to thank everyone responsible for delivering your nighttime depravity: Great Scott, Krisz Klink, Zziks, Mindy, Kermit, djdead, and tribalsoul.

Vendors would like to thank Roamer for leading the charge and making the vendor area what it is today. Dan (wad) is an awesome second and deserves high praise. Thank you to redbeard, AlxRogan, Latenite, PushPin and CrYpT for the great support, hard work and putting up with my way of doing things. A special thanks goes to Nikita, Charel and Will for coordinating everything behind the curtains. We appreciate everything all the other groups do to make DEF CON happen. Finally, thanks to DT for having us!

effffn and the DEF CON community would like to thank the NOC team: Mac, Videoman, #Sparky, t3ase, Rukbat, Booger, Naifx, and Arhawk. These guys devote their DEF CON experience to hard work during the entire week including lots of planning throughout the year so everyone can interwebs and watch the talks in their hotel rooms during the show.

Agent X would like to thank the Speaker Operations staff; Bitmonk, Bushy, Cars, Cli, Code24, Crash, Gattaca, Goekesmi, Jinx, Jur1st, Mnky, Notkevin, Pardus, Pasties, Pwcrack, Quadling, R!Sk, Scout, Shadow, and, Lord Vaedron, These awesome individuals come together as a team every year to help the speakers through a DEF CON speaking experience. They work hard, party hard, and always managed to keep it fun. Thank you for another year of supporting DEF CON and the community.

QM Stores is brought to you by Blood, Sweat, Miracles, Self Abuse, The Grace of Bob, Accident and often Lunchtime. With the help of ETA, RijilV, Wasz, Buttersnatcher, SunSh1ne, Minor Mishap & Major Malfunction. We would like to thank all Humans for giving us a reason to come to this beautiful oasis of calm and tranquillity, here in... Oh, wait... Never mind. We would like to thank all our fellow Goons for making our life easy by always reading the label and returning our shiny toys in their original packaging, or what's left of them in an easily disposed of liquid-proof container. We love you all. Good night & Good luck.

Secret would like to thank the Swag Goons (Lisal33, furysama, SinderzNAshes, Diami03, Daedala, gLoBuS, gingerjet, spiggy, Dasha, Magnar, themikeconnor, Pelican, Mr.Katt, Skyfall and 10rn4) for all their hard work, and all the other teams for their support!

Registration would like to thank: Tyler and Matt; TW; John D., for distracting the crazies; the Info Booth team; the goons who tirelessly manage the lines and stanchions; and the attendees, for their patience.

The registration team is: Crackerjack, APT, apebit, 6Q, Phear, falconred, Jenny O, Temtel, Model-A, and cstone.

Stealth would like to thank the CTF staff and contest goons, the security goons for their tireless efforts, Charel for making impossible things possible and DT for his general awesomeness in creating this thing we call DEF CON.

Blak would like to thank s0ups, w4ld0, and Salem for their work with the DC Groups effort, and to all the DCG POCs who organize their local efforts. A special thanks goes to russr for his helpful guidance when asked - and to Will for making sure the DCG Challenge [DC20] badges made it to every group which participated. Happy hacking and have a great DC 22!

Melloman and Littlebruzer would like to thank the InfoBooth goons for for spreading all the misinformation -- Jerel, jixion, Fran, jimi2x, Jenn, Sanchez, ACR0NYM, TC, Scurryfool, Krav, Algorythm, edison, Littleroo,

1C0ju3r would like to thank all those who live the Production motto: Credo Quia Absurdum est! Kampf, KillerSpud, Doc, Buttercup, Hazmat, Noise, rewtd, <textress> and Betsy. Our Digital Visionaries Anch, / astcell. Julia and Medic. And our extended circle with Russr. And never forget...there be Dragons here!

Grifter would like to thank, Stumper, l3d, and Metacortex, for helping keep the Parties and Villages going, thus ensuring DEF CON attendees had somewhere to feed their passions during the day, and drown them in liquid and sound at night. Thanks guys!

Nikita wishes to thank the CFP Review Board and the accepted speakers for their countless hours of hard work. Thanks to Neil, Tottenkoph, GBF Highwiz, Roamer, Jericho,"I know Neil"- "Hands on Top" Integroll, Jar Jar, and DT. Much love to Lockheed and all our Goon family.

Neil would like to thank: Nikita, you always have my back. LosT, Ellen, Mar, Sleestak, Supafraud, y3t1, DT of course, and all who participated in the Art Contest.