
def con 21

WELCOME TO DEF CON 21!

I have a bit of a confession to make. We tried hard to find a clever image for a theme for the con this year that didn't have anything to do with black jack, poker, "finally being legal" and old enough to drink. We really did. After a month of fighting against it I gave up, and instead we have embraced the 21. From the badges to the pub crawl there is no denying it! The one thing I wanted to do but it ended up being too complicated was to produce legit DEF CON poker chips.

Special things to look for this year is the screening of the DEF CON Documentary Thursday and Friday nights, the continuation the tradition we began at 20 of the music to hack by audio compilation CD - this year we have some new artists, as well as past favorites.

You'll notice a slight change to the schedule this year. The talks are 5 minutes shorter, forcing the speakers to focus a bit more on their core messages, as well as letting everyone have more time between tracks to socialize a bit and not feel so rushed.

We rearranged the floor plan to make more space available to the popular hacking villages, including the new Tamper Evident Village (TEV).

The challenge we face every year is how to get people to break free from the large speaking rooms and meet people in smaller spaces. The villages have been great at that, and this year we grew them as much as the space allowed. We are also trying new stuff with the pub crawl, mini party spaces of a few hundred square feet, as well as more contests focused on forensics and defense. Next year for 22 we will launch a forensics village to formalize this.

Finally I have something serious to say. I have been observing and participating in the community for a long time, but something about this year is different. There has been a tension and frustration level that I have never felt before.

The constant dripping out of revelations, something I expect to continue on a build up to the con and onwards after it, has contributed to a level of mistrust and anger I've never seen directed toward the government. During the "crypto wars" of the 90s there was a bit of this, but nothing to the level happening now. The more paranoid of us all assumed programs such as these existed, but once they were actually confirmed people began acting differently. They existed last year, and they will exist next year, but that confirmation has changed the dynamic. I couldn't ignore it or pretend everything is normal. That wouldn't be healthy for me or for the community. Not everyone agrees with what I said about asking the feds to consider taking a time out this year, and I respect that. But the balance has swung radically in favor of offense, and defense seems futile to some right now.

When all of your favorite software, services and infrastructure are wired to be monitored from the beginning, you've got to be wondering where this all leads. How do we restore that balance? If it can't be restored what do we do?

So here we are, after 21 years, at the beginning of a new era. Somehow I don't think the cloud or big data are going to save the day and restore trust to all the systems we depend on. We need to do that ourselves by continuing to research vulnerabilities to better secure our systems, and to encourage manufacturers to fix their bugs and reveal their privacy practices, and not to play word games with what they do with our personal data.

I hope everyone enjoys the con, learns new stuff, and inspires others to step outside of their comfort zone and experiment with a new technology. Also take some time to talk to others about how we as a community should move forward, I think some introspection will be good for us.

—The Dark Tangent

Contents

The Network

DefCon : Type: Open / 2.4 and 5 Ghz

DefCon-Secure : Type: WPA2/ 802.1x

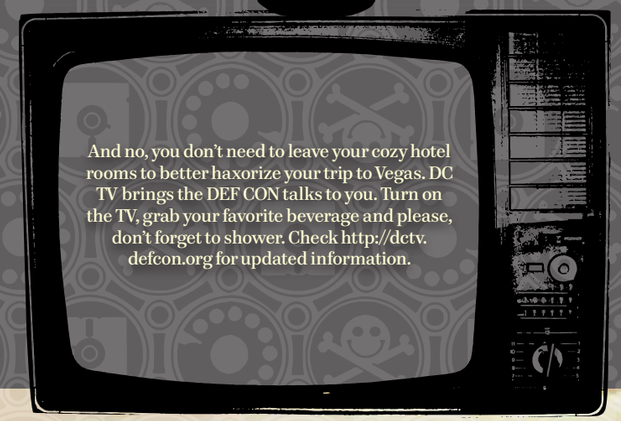
No different that the past few years, the DEF CON NOC works hard to provide you the internetz via WiFi access throughout the Rio convention center. There are two official ESSIDs: the "confined" one with encryption and cert/user-based authentication and the USDA not-so-approved "free-range" one. All of your base are 802.1x compatible these days, so configure it properly and enjoy the GHz. Create your user and download the digital certificate at http://wifireg.defcon.org

And always, our special thanks to the super-reliable NOC staff who keep things running every year while (and actually before) you are enjoying the con: Lockheed, Heather, Mac, EFFFFN, Tabkur, Videoman, #Sparky, t3ase, Arhawk, Booger and Naifx . Remember, without them you would actually have to have real conversations with people.

Check http://www.defconnetworking.org for stats, data and updates about the network during and post-con, or follow us on our new Twitter : @DEFCON_NOC.

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

DEF CON TV



And no, you don't need to leave your cozy hotel rooms to better haxorize your trip to Vegas. DC TV brings the DEF CON talks to you. Turn on the TV, grab your favorite beverage and please, don't forget to shower. Check http://dctv.defcon.org for updated information.

THE BADGE

A hacker in the Vegas desert…sounds crazy, no? But here at our little conference you might say every one of us is a hacker. Trying to scratch out a leet, simple 0day without breaking too much crypto. It isn't easy. You may ask, why do we stay up all night coding if it's so difficult? Well, we stay up because we're hackers. And how do we keep our focus? That I can tell you in one word…predisposition!

Because of our predispositions, we've kept our focus for many, many years. Here at Defcon, we have predispositions for everything. How to sleep. How to eat. How to work. How to wear clothes. For instance we always keep badges around our necks and always wear black t-shirts. This shows our constant devotion to gaining knowledge. You may ask, how did this predisposition get started? I'll tell you. I don't know.

But it's a predisposition, and because of our predispositions, every one of us knows who he is…

Ok enough personal fun- this year I went for a non-electronic-electronic badge. Fabricated printed circuit boards that are stand-alone art/crypto puzzle. I'm going for a tick-tock, every other year electronic badge cycle. Most of the feedback from last year requested another non-electronic badge and badge challenge. (Believe it or not we had much more participation in the badge contest the titanium year than last year's badge.)

It was quite a challenge getting PCB layout software to function as graphic design software, and the fab house didn't quite know what to make of the gerbers I was sending to them. I love using systems for things other than their intended design like that.

The mechanical watch movements in the Uber badges this year are homage to my grandfather, who was a watchmaker. I hope we can all approach our craft of security with as much precision, skill and honor as grandpa had.

Also, with DT's permission, I've decided to break with a few Defcon traditions this year. If you'd like to know what those deviations are, come to the opening presentation- but here's a hint: forewarned is fore armed.

Just to get you started:

www.defcon.org/1o57/dc21/?

(Was the hint above shaky enough? Have fun, and talk to some people. Break your predispositions!)

—Ryan "LostboY/1o57" Clarke

Goons

Goons make DEF CON happen - almost 300 in total!

Goons come in various sizes and varieties Some goons help with coordinating speakers, some with registration, other with contests or entertainment, but all are goons! When spotting a goon you will notice they come in two colors, red and black. Red shirt goons are there for con safety, coordination, and dealing with any last minute emergencies. Black shirt goons are the teams working behind the scenes to make it all happen in their specific area of expertise.

Goons are friendly people and donate their time to make DEF CON happen because they care about the community are into some aspect of the technology. All Goons are there to make sure everyone has a good time and help with any questions you may have.

If you see someone with a goon badge and shirt on they are on-duty and ready to help. If they are wearing a goon badge but NOT a shirt that means they are off duty and just hanging out at the con like everyone else.

MEDIA21 SERVER

The media server from last year is back! Upload and Download! WarEz AlerT!

Point your browser at ftp://dc21-media.defcon.org!

What you will find:

Images of this year's conference materials, music, art and pictures as well as everything we can find from years past as well as a limited reading directory and other security odds and ends. Grab what you want, and please upload and share what you have related to the con. We would love to get pictures, write ups, wordlists, whatever you may have!

And for those of you in a rush we will also have physical wired LAN connections to the media server at the Info Booth where you can plug in, get a DHCP address, and start leeching directly. Play nice!

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 Contest Area. We are here to help you enjoy the Con by providing the latest updates and information that is DEF CON. Got a good rumor, we might help spread it. Keep two things in mind...1) dumb questions get dumb answers, 2) sometimes we just don't have the answer immediately but we know how to get it.

SERVICES FOR YOU:

- http://updates.defcon.org (best way to stay current)
- Directions
- Twitter posting
- Contest results / updates
- Latest schedule displayed
- Program viewing
- Donation point for the EFF
- Passport stamp
- Humiliation (as needed)

PRISM

S2'1E01: LEAKY FAUCET

AIR DATE: Thursday 8.1.13, Track 1 (Rio Pavillion 8-11), 9pm-2am

FADERHEAD

BLAKOPZ
MISS DJ JACKALOPE
EDWIN SOMNAMBULIST
THE GOON BAND

S2'1E02: KEEPING IT META

AIR DATE: Friday 8.2.13, AMAZON P+O, 9pm-2am

BIL BLESS
AU5 + FRACTAL
THE_AUDIOPHILES
PSYMBIONIC
DJ ZERO ONE

S2'1E03: SHEARING THE PIG

AIR DATE: Friday 8.2.13, AMAZON T+S, 9pm-2am

SCHLAUTING THOMAS
MODEM GIRL
SOUL BUTTON
ZACK BARBIE
DJ%27

**** TIMES AND LINE-UP SUBJECT TO CHANGE ****
VISIT DEFCON.ORG FOR THE MOST UP-TO-DATE SCHEDULE

BREAK

S2'1E04: SNOWED IN!

AIR DATE: Friday 8.2.13, Track 1 (Rio Pavillion 8-11), 9pm-2am

bt

LEFT / RIGHT
GREAT SCOTT
MITCH MITCHEM
PROJECT MAYHEM

S2'1E05: TRANSIT LOUNGE

AIR DATES: THURSDAY 8.1.13 - SUNDAY 8.4.13, MIRANDA, DAYTIME

ESCAPE AND WAIT WITH soma fm

S2'1E06: BUG INFESTATION

AIR DATE: SATURDAY 8.3.13, MIRANDA, EVENING

CODAME

ART + HACK
INSTALLATION
PARTY

CONTESTS

Black Bag

On Twitter and around con space (contestants seeking clues)

12:00 - 17:00 on Friday in the Contest Area

13:00 - 17:00 on Saturday in the Contest Area

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 (three players each... and more than 7 teams may also be possible) to tell us where this target individual can be found will get to participate in the main round 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 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 the same setup of gear (provided by the contest staff) in order to keep things fair. Follow us on Twitter to stay abreast of all that is planned!

Beverage Cooling Contraption Contest

10:00-14:00 Friday - Contest is at 12PM on Miranda Patio

The BCCC is in its 9th year running! "Beverages" are cooled by contestant designed contraptions in a feat of ingenuity, skill, and sometimes luck!

Capture The Packet

Friday 9:00 – 19:00, Saturday 9:00 – 19:00, Sunday 9:00 - 12:00 in the Contest Area

Capture the Packet "CTP" is a one hour game were teams of two compete by monitoring the "live" CTP network traffic in the ultimate network forensics and analysis challenge. Whether your are a Network Samurai or net-admin that focuses on the defensive arts, this game is for you; 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 puzzles and score points. Overall high scores move to the finals on Saturday evening where they have a chance to compete for amazing prizes. You can register your team of two on-line at "CaptureThePacket.com" or at the CTP table in the contest area. Once you register stay tuned by following our Twitter feed, Facebook and Web pages for dates and times your team will compete, as well as prizes that will be awarded.

Communicating On A Different Frequency

In the Contest Area

Exploit the previous years human badge to communicate messages via encrypted rf signals(in order to complete the event you must prove that you can communicate encrypted messages using the original and non physically modified def con 20 human badge(this is purely a software exploit) an exception to the old badge is the new badge. I will demonstrate a non rf encrypted message and then a contestant will have to exploit the rf component on two badges and demonstrate communication between said two badges. The only rule is you can't modify the badge physically in any way or form to be able for a chance too win. If your not first your last! As an added bonus the first 25 participants will receive a system failure poster, then link to the poster is posted here. http://m.flickr.com/photos/tommietheturtle/8632336951/lightbox/ The first five participants will receive the website urls poster image and have an option at 1 of 5 signed limited edition poster prints of the image here http://m.flickr.com/photos/tommietheturtle/8391333152/in/set-72157633199875115/lightbox/

Crack Me If You Can

24:01 AM Friday, until 24:01 AM Sunday in the Contest Area (while open)

Crack the most, hardest passwords in 48 hours, win fabulous prizes and bragging rights! 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.

Crash And Compile

Saturday 20:00 - midnight/1:00 Contest Area Stage

"A programming contest crossed with a drinking game. What can possibly go wrong?" 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. In previous years during this distinctive competition contestants have gone to such lengths as to weld basket-ball sized metal dice to choose their programming language by chance, have written their own language to solve the problems, and have chosen such unorthodox development environments as the clearly superior palm pilot, to a functioning robotic PDP-11/23 complete with antiquated green screen terminal... and in the most audacious of cases, have won the competition without looking at the screen. Do you have what it takes to Crash And Compile?

DEF CON Scavenger Hunt

Fri: 1000-1800 Sat: 0800-1800 Sun: 0800-1200 in the Contest Area

The strangest, loudest, most chaotic and quite possibly the most infamous game at DEF CON, the Scavenger Hunt.

Exploit Hackathon

In the Contest Area

Exploit Hackathon 2.0 DC21 [2013] Exploit Hackathon will return this year and the rules have changed. For too long we have suffered in silence while rude multitudes have screamed on our screens. It is time to take action, to heed the call and end the suffering of a misbegotten tool too easily abused by the masses. This can continue no longer. The time has come and the battle lines have been drawn. In short, it is time we declared WAR on the CapsLock button. For the next 72 hours you are an agent tasked with making a difference in the battle of the noise. Your objective: To make a single decisive strike and render the capslock key useless. You may disable, redirect, reutilize or otherwise fsck this button into oblivion. You must: Document your plan of attack Code a virus (utility) to do your dirty work Demonstrate a working copy of your construct Provide both the working utility and a cleanup tool (just in case) Submit your Code. To win: Be creative; the better and more useful your utility the more it will be remembered. Be aggressive; you should have a plan to self propagate your "tool" [A 0-day here will get you considered but will not guarantee a win] ** Have Fun. The more interesting, useful, entertaining, wacky your utility is, the more you put into it, the more likely it is to be noticed. ** Code for Zero-Day attacks will be withheld until the attack can be responsibly disclosed to affected vendors. It is possible the revelation of such an attack may be eligible for a prize. Any such eligibility will be forwarded along with the exploit. Exploit hackathon entries will be judged by notable infosec figures who must be impressed to decide a winner. Last year no one was able to claim the prize, this year will it be you?

Hack the Planet

Friday 0001 hours till Sun 1159 hours

Who can produce the biggest benefit to society as a whole. Donate, give, hack, just have it benefit more people than you.

Hacker Pyramid

Friday & Saturday night before Hacker Jeopardy

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 ???? ---- we don't know, there's no more penny!

Hackers Against Humanity

Friday 10:00 Round 1: 60 min (approx.) 11:00 Break: 30 min 11:30 Semi-final: 60 min (approx.) 12:30 Break: 30 min 13:00 Final: 60 min (approx.) 14:00 BTD

From the same evil genius minds that bring you theSummit, Vegas 2.0 presents: Hackers Against Humanity! Conspired from "Cards Against Humanity", we have collated a deck with the special smell of hackers added. 1 part social engineering and 2 parts being a horrible person; mix and serve. This single elimination style contest will pit - 80 total contestants across 10 simultaneous games - players against each other for one champion hero. Each round, one player asks a question from a Black Card, and everyone else answers with their funniest White Card. Dealer picks the best card. Most rounds won by the end of the deck wins and progresses onto the next round.

Hackfortress

Fri open-close, Sat 10:00-20:00, Sun 10:00-15:00 in the Contest Area

Hack Fortress combines elements of two classic contests; a multidisciplinary hacking contest and a Team Fortress 2 LAN party. Calling upon the best of both, Hack Fortress will pit teams of players against one another in a dual-challenge event over the course of two days at DEF CON 20. So, how does this Hack Fortress thing work? Two teams (6 Teamfortress 2 players, and 4 hackers) team up to get as many points as possible in a 30 minute time period. As players hack their way through the challenges, they will not only earn points for their team but will also be gifting their TF2 players bonuses and perks to give them an edge. A solved challenge may result in 15 seconds of critical hits or something else as devious. The same is also true for the TF2 team--without a flag or point capture in game, it may be impossibly hard to hack through a particular challenge. Without coordination and cooperation between the two elements of a team, neither will be victorious.

The Most Significant Bit

In the Contest Area

The Most Significant Bit (MSB) is a King of the Nerds style game for Hackers. 16 candidates will be selected from video auditions posted on YouTube, eventually being narrowed down to the Final Two. Who will win the crown, and be noted as the Most Significant Bit? This contest will begin Thursday evening, with the field of contestants being cut in half, each day. Primary

CONTESTS

eliminations will be held each evening, with secondary events held during the day. Challenges will be created from hacker/maker interest areas.

Network Forensics Puzzle Contest

9:00 - 18:00 in the Contest Area

Get ready for the ultimate forensics challenge! This year's Network Forensics Puzzle Contest is the first in our new "P.I. Series." Your evidence will include: - Blackhole Exploit Kit 2 infection traffic - VOIP (SIP) traffic - GPS data - Android filesystem dump (yep, it's more than just network forensics!) - MMS video messaging ... and more! Follow the trail of dead bodies, leaked documents, mysterious diseases. Featuring Jack Stone (private investigator), Victoria Jensen (the suspicious wife), a strange blackmailer, and the CEO of a large DoD contractor. Can you unravel the twisted web they weave... or will the murderer get away?

Ninja Cyber Target Range

8:00 to 20:00 in the Contest Area

1. Novice or Newbie range - Flat network no defenses simple targets, for each target they "own" receive a ticket.

2. Advanced range - have a perimeter router with a weak ACL they have to penetrate, then a public DMZ and firewall with a private DMZ. - The DMZs will have default installs of the latest OSs - Server 2012 - Server 2008 - OpenBSD 5.2 - Ubuntu 12.10 - internal network that is accessible from one of the DMZs, they will have to own a box then pivot to the - internal network, internal net will have default installs with a few hardening steps implemented - ticket for each box owned The intent of the advanced range is to allow contestants to go against an environment that is similar to any external penetration test that is conducted. The layered architecture will present a challenge, but there will be weaknesses there so they can get into the first DMZ, as they progress through each layer it will become more difficult to go further. Additionally, there will be a multitude of operating systems that they will encounter, so it will take an extensive skill set to "own" the boxes. The premise will be the OS many have considered to be one of the most secure (OpenBSD) will be alongside the new and latest offerings, which one will survive and which one will be toast! Or, will no one "own" an OS that is not purposely made weak?

Pimp my Rascal

Information Booth open Friday 10:00 - 17:00. Contest begins 13:00 Saturday and ends 14:00 Saturday

I heard you like shiny lights, so I took your Rascal Chair and put glowy crap all over it so you can look hip at the con! Contestants will get until 1:00PM Saturday to Pimp out a Rascal Chair (or competing vendor). * Cost of pimping is not to exceed $500. * Rental chairs allow to compete * All "mods" must be proven not to damage a chair (I.e. if you were to remove everything, you would never know the chair was modded) * Chair must fit one person after mods * Chair must run on it's own battery and motor after mods

Project 2

Friday 9:00 - 20:00(ish), Saturday 9:00 - 20:00(ish), Sunday 9:00 - 14:00 in the Contest Area

Project 2 is a drop-in contest for novices to experts to hack on while at the con. It is designed for contestants of all skill levels to stop, play, and enjoy a challenge without prior registration or commitment for the rest of con. Unlike most contests, we will help you if you get stuck.

Social-Engineer Capture the Flag

Friday 8:00 - 7:00, Saturday 9:00 - 8:00, Sunday 10:00 - 1:00 in Palma G-H

This truly unique event will challenge you and test your abilities to use social engineering skills to gather small amounts of data from unsuspecting people over the phone. Testing your abilities to use basic social engineering skills in front of a group of your peers and prove you are "The Deadliest Social Engineer"

Social-Engineer Capture the Flag for Kids

Friday evening, Sat 8:00 - 18:00 in Palma G-H

This contest is designed to use a blend of social skills, password and cipher cracking, lock picking, and good old-fashioned social engineering to accomplish a set of challenges. Each challenge must be completed in order to move on to the next until the first team to complete is declared the winner.

The DEF CON DarkNet Project

24/7. No in-person component, it's all on-line.

An ARG/MMO run by a Daemon sending players on quests to learn new skills, meet new people and do new things.

https://dcdark.net

The Schemaverse Championship

All con - booth manned during Contest Area Hours

The Schemaverse is a space-based strategy game implemented entirely within a PostgreSQL database where you compete against other players using raw SQL commands. Use your SQL skills to interactively command your fleets to glory during this weekend-long tournament for the database geeks. Or, if your PL/pgSQL-foo is strong, wield it to write AI and have your fleet command itself while you enjoy the con! This year, we are also hosting qualifying rounds leading up to DC21 at various other conferences and groups. At each of these qualifiers, the winner gets a free badge (from us) and a spot in the championship round. The format of the contest this year at DC21 will be another additional qualifying round from Thursday to Friday, and the final championship round Saturday to Sunday.

Wall of Sheep

Friday 9:00 - 19:00, Saturday 9:00 - 19:00, Sunday 9:00 - 12:00 in the Contest Area

The Wall of Sheep is an interactive demonstration of what can happen when network users let their guard down. We passively observe the traffic on the DEF CON network, looking for evidence of users logging into email, web sites, or other network services without the protection of encryption. Those we find get put on the Wall of Sheep as a good-natured reminder that a malicious person could do the same thing we did . . . with far less friendly consequences. More importantly, we strive to educate the "sheep" we catch—and anyone who wants prevent leaks in the future. The Wall of Sheep will be hosting several workshops such as Network Sniffing 101, and Advanced Traffic Analysis. Classes will be through-out the conference, check the schedule at the Wall of Sheep for dates and times. In addition, this year we will be launching an educational series utilizing the Capture The Packet (CTP) game engine to introduce people to the concepts of network forensics and traffic analysis. Come be part of history and capture traffic at the "Wall of Sheep" for yourself.

warlock gam3z

All con - booth manned during Contest Area Hours

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.

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.

We hand out prizes to the top 3 finishers, in the event of a tie we drill down to the timestamp and base it on who got there first.

Our social media event pages: https://www.facebook.com/Gam3zInc https://twitter.com/Gam3z_Inc http://www.youtube.com/user/Gam3zInc

WiFi Sheep Hunt

Friday 9:00 - 18:00, Saturday 9:00 - 18:00, Sunday 9:00 - 12:00 in the Contest Area

Calling out all you wireless sniffing gurus, Hackers and those that are not-so-much, the "WiFi Sheep Hunt" (c) in its second year provides attendees with a Quest – A DEF CON Wide search for all sorts of wireless emitting devices, we don't want to give it away, however if it can transmit a RF signal, chances are it might be on your quest, but that's not all, you will first need to solve a encoded riddle, then locate certain devices, which will create a key for accessing the wifi.sheep.hunt network, where you will need to utilize further hacking skills. For complete contest rules and details of the Quest, Visit the Wifi Sheep Hunt website www.WiFiSheepHunt.com and game day visit the WiFi Sheep Hunt Table and obtain the Official Quest directive. Various prizes will be awarded for first, maybe second and not likely third place, and of course *Standard rules and disclosure for DEF CON apply.

Wireless Pentathlon

Friday 10:00 - 20:00 Saturday 10:00 - 20:00 Sunday 10:00 - 16:00 in the Wireless Village

There will be contest rigs sold at Simple-WiFi (DEF CON vendor) to support those that don't have everything they need. There will be clues to the tools necessary as we get close to the contest, and all updates will be over Twitter and DEF CON forums. All contests minus the long distance shootout will be a timed flag, less points once the first person pulls a flag

Friday 11:00 - 15:00 - Long distance signal strength Shootout

Friday 16:00 - 20:00, Saturday 10:00 - 15:00 - Hide and seek

Saturday 16:00 - 20:00, Sunday 10:00 - 14:00 - WPA2 cracking

Saturday 16:00 - 20:00, Sunday 10:00 - 14:00 - Fox and hound

Saturday 16:00 - 20:00, Sunday 10:00 - 14:00 course *Standard rules and disclosure for DEF CON apply.

CAPTURE THE FLAG

Brought to you by

真の会社

Legitimate Business Syndicate

HELLO AND WELCOME TO DEF CON 21.

We're Legitimate Business Syndicate, and we're proud to have been selected to pick up the reins on DEF CON Capture The Flag from Diutinus Defense Technologies Corp. (NASDAQ: DDTEK). We have an exciting game planned this year that should be familiar to CTF veterans but still exciting and distinct.

WHAT IS CAPTURE THE FLAG?

DEF CON Capture The Flag is a competitive live-fire hacking competition. Each team starts with an identical set of network services they must defend from other teams, while at the same time using their understanding of these services to attack other teams. Services could be anything from a simple rolodex/contact 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 is the offensive game. Protecting flags from exfiltration while at the same time keeping them available for uptime checks is the defensive game.

OUT WITH THE OLD

We've competed in dozens of CTF games, including several years at DEF CON. We've seen enormous teams qualify and win in the past, and believe that's led to a bit of an arms race. One of our goals is to make small teams viable again. We strongly believe in smaller, more elite teams, and hope teams will cooperate with us. We've worked on rebalancing the game to make large teams less valuable, and asked for your cooperation in bringing smaller teams to the game.

IN WITH THE NEW

The services we've built this year are designed to be deeper and more complicated than previous years. While we're keeping most of them a surprise for when the game opens Friday morning. Do brush up on your non-x86 architectures. Maybe, get to know an obscure operating system, learn how to own stuff Axel Foley style, and most of all be flexible.

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 don't interrupt hackers at work, don't photograph screens, and above all be respectful and not a jerk. If you do have questions about the game, definitely talk to a member of Legitimate Business Syndicate, and many competitors may be happy to talk when they're not engrossed in the game.

QUALIFYING

There are several ways to qualify for competition in DEF CON CTF. A challenge-based (solve problem, get points) qualification round is hosted online months before DEF CON, with the top ten or more teams moving on to compete here in Vegas. The previous year's winner is always invited back to defend their title, and winners of other select competitions online and around the world are automatically qualified to compete here in Vegas.

We'd like to shout out to Kenshoto, DDTEK, and CTF organizers around the world for shaping the game, and we hope that our competitors and spectators enjoy what we have to offer. Game announcements will be posted to https://twitter.com/legitbs_ctf . We'll keep a scoreboard on the wall in the competition room, and we'll announce final results during DEF CON closing ceremonies.

Thanks,
Legitimate Business Syndicate
https://legitbs.net

DEF CON: THE DOCUMENTARY

Showing at 17:00 Thursday Night in Tracks 2-3, 20:00 Friday in Track 2

Get your digital copy on media.defcon.org, free of charge.

We also have the special edition standard or deluxe packages available at the swag booth or on hackerstickers.com

In February of 2012, I was in Helsinki traveling with Rachel Lovinger when I was contacted by long time goon Russ Rogers. His question was simple: since DEF CON was coming up on the 20th anniversary, and I had been both a long-time attendee and a director of several technology-based documentaries, would I be interested in doing a documentary on DEF CON and its 20th year?

I said I needed to think about it, but I really didn't have to think that long.

A year and a half later, I put the finishing touches on a two hour movie and an hour of bonus footage, having spent the previous 18 months planning, shooting, organizing, editing, and just generally living this movie day in and day out.

DEF CON: The Documentary is having its premiere at the only place that felt right: DEF CON 21. We'll be showing the movie on Thursday and Friday night, and Rachel and I will be giving a presentation on Friday afternoon about how this crazy project was pulled off.

This movie would not have been possible without our incredible crew: Rachel, Alex, Drew, Rick, Steve, Eddie, and Kyle. And Russ Rogers has been an incredible force-of-nature, helping move the production along every day. A big shout out to Jeff for funding this project while not seizing editorial control along with the checkbook. He let us run free, and I think the film shows that.

While we weren't able to cover every last aspect of DEF CON (and who really could?) I think you'll find there's something for everyone in the movie. It was done out of love and respect for this incredible conference and the people who make it happen. I hope it brings a whole new appreciation of the special event we have here every year.

See you at the movies!

-Jason Scott

EVENTS

Forum Meet

16:30 to 02:00 in Amazon H&J.

The "Forum Meet" offers the DEF CON online community the opportunity to meet and put a face to the names and avatars they see year round on the DEF CON forum. It's a place to see old friends and make new ones. If you are a forum participant or "lurker" stop by and say hello.

If you are new to DEF CON this is an excellent opportunity to become part of the year round DEF CON experience. This event gives you, the new DEF CON attendee an opportunity to join in, and gives you a chance to ask questions about the Con that you may not have other opportunities to get answered elsewhere. Meet the people who run the forums, goon the con, and have been around since time immortal. (or so it seems)

This year's forum meet we will be bringing back DEF CON Trivia,so come in for a chance to win some awesome swag. You don't have to be old school to play, new comers will have a chance to win as well. We'll also have some interesting party surprises planned as the evening goes on and a special performance by DEF CON's very own Goon Band RECOGNIZE.

There will be flashy lights, and if you have some, bring them, since this year's party host decided to skimp on the décor budget in favor of fun and prizes, we need you to light up the room for us. A special prize will be awarded to the person with the best blinkie-shiny-ELWire contraption attached to them. So, if you're prone to seizures, you might want to steer clear.Hacker Karaoke

Hacker Karaoke

Thursday 9:00 - 2:00, Friday 9:00 - 2:00 in Amazon C-D

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.

Queercon

Social Mixer: Friday & Saturday - 16:30 DEF CON Chillout Area

10th Anniversary Pool Party: Friday - 20:00 VooDoo Pool Area

Queercon is turning 10 this year, and we're going to celebrate!

Friday and Saturday 4:30 PM come hang out, grab a drink and meet other LGBT hackers and their friends. Look for us in the DEF CON Chillout Area. It's a great low key way to socialize and meet other people.

Friday at 9PM Queercon is kicking off our 10th Anniversary with a big pool party. Come party with us in the VooDoo Pool Area, great DJs, dancing, and more.

Queercon is open to all LGBT hackers and friends. No bad attitudes and no invitations needed - come as you are.

Find out about all of the queercon activities at queercon.org or follow @queercon

IOACTIVE Freakshow

Saturday night at the pool

IOActive is once again pleased to present the Freakshow at DEF CON! Open to all attendees, friends, and freaks alike - this year's party promises to stretch the imagination and provide fun for everyone.

Join us at the Rio pools on Saturday night for live music by DJ Keith Myers and crew, mind bending fire acts, a twister of epic proportions, tasty libations, and much, much more!

Art for EFF

8:00 - 18:00 in the Contest Area

I create art for DEF CON with Neil and sell some of it in the form of shirts, hats, prints, and originals to raise money for EFF. I even do some custom work on badges and laptops (and sometimes people) with Sharpies.

Be the Match

9:00-17:00 in the Contest Area

Registry drive for the Be the Match National Bone Marrow Registry

Cycle Override DEF CON Bike Ride

Fri 6:00

JP Bourget and Bruce Potter are running the 3rd annual DEF CON bike ride - in addition are cycling across the USA to DEF CON to raise money and awareness of the EFF. Come join us for a day on the way to Vegas or Friday morning of DEF CON at 6am for a 20 mile loop out to Red Rock.

Ham Radio Examinations

Sunday 12:00-15:00 in Palma G-H

Come to (near) the Wireless Village on Sunday between 12pm and 3pm, where we'll be giving ham radio license examinations so that you, too, can (legally!) use 15,000 times normal WiFi power, read RFID tags from half a mile away, talk to satellites, and bounce signals off incoming asteroids. (Yes, we actually do that.) The FCC makes us charge $15 for this (we don't keep any of it), but we'll take cash or a check; that fee covers your first 10 years of amateur license registration, as well as the ability to take the exams once for all three license classes: Technician, General, or Amateur Extra. Go home with a better memento of DEF CON than just a hangover and a pile of t-shirts!

Mohawk-Con

Friday-Sunday in the Contest Area

Shavin' skulls and takin' moneys. Donations go to Hackers for Charity, Competing HackerSpaces, and the EFF.

BloodKode

In Palma G-H

DefCon is not only an opportunity for networking, learning, socializing and partying; it is also an opportunity to SAVE A LIFE!

For the past 3 years BloodKode has been an active part of the conference- a chance for participants to donate a pint of life-saving blood.

This year we have 3 days:
Aug 1 Thursday 12noon – 5pm
Aug 2 Friday 9am – 5pm
Aug 3 Saturday 9am – 5pm

Look for the signs to "BloodKode"

Qualifications for HEROISM:
· 17 years of age or older
· Feeling well and healthy
· Photo identification
· Tattoos must be 1 year old to qualify for donating depending on state in which applied
· Please EAT before donating and try to drink LOTS of WATER .

To schedule an appointment (walk-ins are welcome, but appointments taken first), click on this link:

https://www.bloodhero.com/index.cfm?group=op&step=2&opid=533849

Thank you for being a HERO!

DEAF CON

9:00 - 17:00 - Interpreters will float throughout the villages and con area.

Our goals are to encourage many Deaf/Hard of Hearing (HoH) hackers to attend DEF CON, help provide those hackers with partial or full services, and provide a place for Deaf/HoH hackers to meetup and hangout. First discussions of reaching out to the Deaf/HoH community for DEF CON 21 started on January 6th, 2013 in a thread on DEF CON forums. Since then, the discussions have focused on identifying services, strategies, and volunteers to make this a success. During the con, we will have a meetup for Deaf/HoH hackers to gather, socialize, and network with each other. Since DEF CON is already sponsoring speech-to-text CART services in the speaker tracks, we are going to provide two live volunteer interpreters for the con. These volunteers are being compensated by funds raised by the DEAF CON Indie Go-go campaign to pay for airfare and accommodations. As of 6/22/13, the campaign raised enough funds to compensate our interpreters. We will be handing out two things: Prizes for those who donated to the campaign (if they chose to pick up their items at the con) and badges identifying attendees as Deaf, HoH, Interpreter, etc. These prizes and badges are being funded by organizers, not by DEF CON in anyway.

DEF CON GROUPS

All around the world, once a month, like minded hackers are meeting up and extending DEF CON year round. These meetings are gathering points for those who wish to share their knowledge with others and continue the spirit of hacking beyond the closing ceremonies of DEF CON. These DEF CON Groups are designed to help people learn new things, meet new people, and to help ensure cohesion in the hacker community as a whole.

With over 270 groups currently active in over 20+ countries, DEF CON groups is alive and well. This year we will have a hackerspace camp to help form new spaces and assist with some legal aspects of forming these spaces/groups. Please check the forum's DEF CON Groups Announcement area for updates regarding the DCGs. If you wish to register new groups head on over to https://goo.gl/hqGQ3. Please be aware the international registrations take a bit longer to verify.

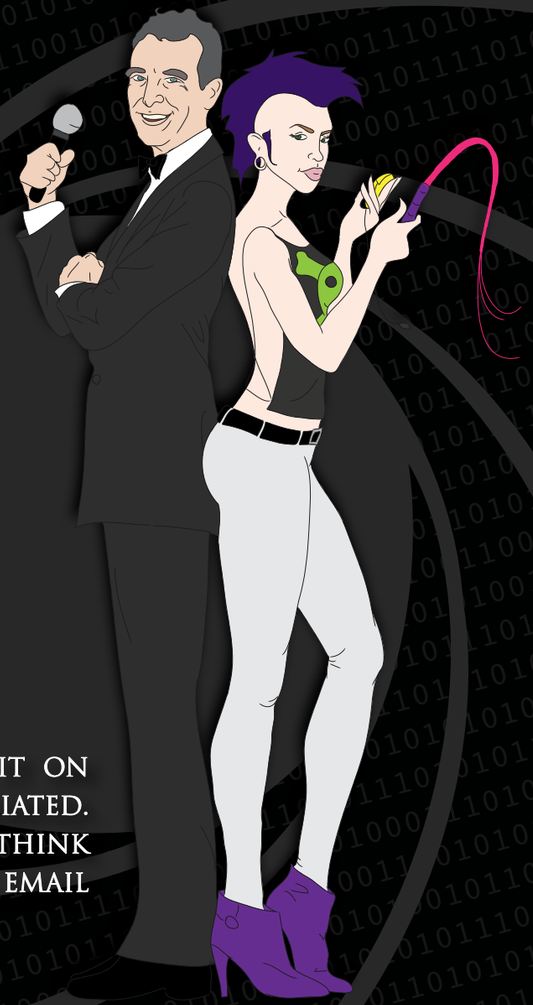
I would like to personally send a shout out to Salem for keeping up with the new registration updates, and to blakbunny and theDns for the clerical work on the backend.

Many changes are coming to the groups this year, so stay tuned to #DEFCON. Have a wonderful DEF CON and Happy Hacking!

-blak

blak@defcon.org

HACKER JEOPARDY



G MARK
VANNA VINYL
BEER BETTY
MISS KITTY
FIZZGIG

PLUS
A SURPRISE GUEST

FRIDAY 8/2 & SATURDAY 8/3 · 9 PM
AMAZON G TRACK 3 · ARRIVE EARLY

THINK YOU KNOW YOUR SHIT? PUT IT ON THE LINE. HUMILIATE OR BE HUMILIATED. WIN COOL SCHWAG! IF YOU WANT TO THINK & DRINK YOUR WAY TO A BLACK BADGE, EMAIL HACKERJEOPARDY@GMAIL.COM

VILLAGES

Lockpick village

10:00 – 18:00 daily in Brasilia 2

Want to tinker with locks and tools the likes of which you've only seen in movies featuring cat burglars, spies, and secret agents? Then come on by the Lockpick Village, run by The Open Organisation Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.
The Lockpick Village is a physical security demonstration and participation area. Participants can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts from TOOOL and Locksport International will be on hand to demonstrate and plenty of trial locks, picks, shims, and other devices will be made available. By exploring the faults and flaws in many popular lock designs, you can prepare yourself not only for possible work in the penetration testing field, but also simply gain a much stronger knowledge about the best methods and practices for protecting your own infrastructure and personal property.

TOOOL
The Open Organisation Of Lockpickers

Wireless Village

1000 – 1800 daily in Brasilia 3

Think you have the skills to crack WPA/WPA2 passwords?

Are you creative and like to roll your own? How about RF antenna's – do you have what it takes to make one that will measure up?

Want to obtain the information you need to pass the Amateur Radio Technician Class license exam?

Done anything with Bluetooth lately?

Get these answers and more at the Wireless Village. Learn about wireless (802.11, bluetooth, software defined radio, and more) and Amateur Radio all in one place at the DEF CON 20 Wireless Village. The one place you will not want to miss.W

Hardware Hacking Village

10:00 – 18:00 daily in Rio Pavilion 3-4

Many Defcons ago LostboY (aka lo57) walked from one end of the DEF CON conference spaces to the other, shouting the question, "Who wants to learn how to build a simple robot?" Eventually a large group wound up sitting on the floor in the contest area building and programming robots. Inspired by that event, Russ Rogers and LosT together organized what would become a regular DEF CON fixture – a dedicated space for hardware learning, hacking, and exploration: the Hardware Hacking Village (HHV) was born. The HHV has been helped along by many, such as Kingpin and a horde of volunteers. As of yet we have not burnt down any hotels with soldering irons.

This year Russ and Ryan (LosT) decided to give a long time volunteer, "A" a chance to function in an administrative lead role in the HHV. Please welcome A and the volunteers he's got helping out this year. LosT, Kingpin, Russ and others will still be around from time to time. Soldering stations will be provided for soldering to the badge or other experimentation.

If you've ever wanted to learn to solder, stop by – lessons are in an open format and ongoing. If you've got hardware skills to share, stop by as well, we welcome those willing to share their knowledge. We will have people on hand to help you get started with microcontroller programming, circuit hacking, and tons of other hardware based hacker skillz. Come void some warranties with us.

Tamper Evident Village

10:00 – 18:00 daily in Rio Pavilion 3-4

Defcon 21 will have the first ever Tamper-Evident Village! For a few years my team (The MFPs / Motherfucking Professionals) has won the tamper contest at Defcon, and this year we'll be dedicating ourselves to running the tamper village alongside the tamper contest organizers. Tamper is a great hobby and one of the relatively unexplored areas of physical security. Come learn about it in a friendly, hands-on environment!

On the bill for the DC21 Tamper Village:

* For your viewing pleasure, collections of high-security tamper-evident seals from around the world.
* Sit-down presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.
* Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags.
* Electronics rework & reverse engeineering stations for working with electronic tamper seals.
* Contest workspaces (space permitting). Sit down in the village and work on your tamper contest box! The village should have a variety of tools you can use to help defeat your box.

We'll also have some take home kits of mechanical and adhesive seals if you want something to take home to practice on.

See you all in the village at Defcon!

DEF CON 21

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

DAY 1 FRIDAY	Classroom in Crown Theatre	Workstations in Antonio's Ristorante	Contests in Antonio's Ristorante	Field Trips at DEF CON 21
10:00 - 10:30	Playing with Your r00tz Badge The Arlens	Code Breaking Museum	Hoff's Crypto Challenge	Welcome and the DEF CON Badge Dark Tangent and L0st
10:30 - 11:00	Meet the VCs - Bring Your Ideas Eileen Burbidge, Ping Li, Matt Ocko and Phil Paul	r00tz Badge Building	Best r00tz Badge Hacks	Welcome and the DEF CON Badge Dark Tangent and L0st
11:00 - 11:30	Watching the TV Watchers Aaron Grattafiori and Josh Yavor	SnapCircuits	Capture the Flag	Hacking Driverless Vehicles Zoz
11:30 - 12:00	Welcome to DEF CON 21 Dark Tangent and Kurt Opsahl	Watching the TV Watchers	DEF CON Badge Secrets	Hacking Driverless Vehicles Zoz
12:00 - 12:30	Meet the Keynote Ambassador Joseph DeTrani	Ask EFF	Scavenger Hunt	Making of the DEF CON Documentary Jason Scott
12:30 - 13:00	I Can Hear You Now Doug DePerry and Tom Ritter	The World Post Office	Name That PLC	Making of the DEF CON Documentary Jason Scott
13:00 - 13:30	101 Zero Days CyFi	Listening to Phone Calls & Texts	Can You Hear Me?	Making of the DEF CON Documentary Jason Scott
13:30 - 14:00	Let's Get a Bill Passed to Protect Your Privacy Nicole Ozer	Find a Zero Day	CyFi Zero-Day Contest	Making of the DEF CON Documentary Jason Scott
14:00 - 14:30	White Hat vs. Black Hat Alexander, Allegra and George Kurtz	Signing a Petition on Privacy	Collecting Signatures	The ACLU Presents: A Year in Surveillance Alex Abdo
14:30 - 15:00	Cell Phone Magic RJ	Movie War Games - PG	War Games	The ACLU Presents: A Year in Surveillance Alex Abdo

DAY 2 SATURDAY	Classroom in Crown Theatre	Workstations in Antonio's Ristorante	Contests in Antonio's Ristorante	Field Trips at DEF CON 21
10:00 - 10:30	Home Invasion 2.0 Daniel Crowley and Jen Savage	Code Breaking Museum	Hoff's Crypto Challenge	A Failure of Imagination Marc Weber Tobias
10:30 - 11:00	Lights, Music and Action! The Joyces	Lockpicking	Lockpicking Race	A Failure of Imagination Marc Weber Tobias
11:00 - 11:30	The Government and UFOs: A 70-Year History Richard Thieme	Controling Lights and Music	Action!	A Failure of Imagination Marc Weber Tobias
11:30 - 12:00	Teenage Hacking in China Philix	Meet the Kegbot	Responsible Root Beer	A Failure of Imagination Marc Weber Tobias
12:00 - 12:30	Stalking a City Brendan OConnor	Meet a Chinese Hacker	Chinese Games	Defeating Internet Censorship with Dust Brandon Wiley
12:30 - 13:00	New Hardware Hacks Joe Grand	FUN Work	FUN Games	Defeating Internet Censorship with Dust Brandon Wiley
13:00 - 13:30	Spy School Chris Hadnagy	Hardware Hacking	Hardware Designing	RFID Hacking: Live Free or RFID Hard Francis Brown
13:30 - 14:00	Making and Breaking the r00tz App Tom Leavy	How Do You Look in Google Glasses?	The Invisibility Cloak	RFID Hacking: Live Free or RFID Hard Francis Brown
14:00 - 14:30	Hacker Jeopardy Kids Winn & Co.	Making the r00tz App	Breaking the r00tz App	Phantom Network Surveillance UAV & Drone Ricky Hill
14:30 - 15:00	Hacker Jeoparty Kids Winn & Co.	Movie Sneakers - PG-13	Sneakers Quiz	Phantom Network Surveillance UAV & Drone Ricky Hill

PRESENTATIONS

WELCOME / THE DEF CON 21 BADGE

The Dark Tangent
Founder, DEF CON and Black Hat

LosT

PROLIFERATION [KEYNOTE]

Ambassador Joseph R. DeTrani
President, Intelligence and National Security Alliance (INSA)

DEF CON 101 [PANEL]

Highwiz
Moderator

PyrO, Roamer, Lockheed, LosT
DC101 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 a n00b or a long time attendee, DC101 can start you on the path toward maximizing your DEF CON Experiences.

You don't need a badge to see the 101 Talks, though some of the content may make it an R Rated movie.

HACKING MANAGEMENT: FROM OPERATIONS TO COMMAND

Lockheed, Roamer, Naifx
So you've been in IT for a while. You've done well. You like your job. When is it time to move on? We aren't talking about finding another job doing the same work. We are talking about making the decision that it's time to bite the bullet and make the dreaded transition into management. For most IT folks management is a dirty word, but should it be? In this talk a senior IT professional, a hybrid engineer/manager and a senior director will talk about the paths that brought them to their positions and why they have chosen to either stay in hands on roles or transition in management roles.

THE NINJANEERS: GETTING STARTED IN BUILDING YOUR OWN ROBOTS FOR WORLD DOMINATION

Beaker, Flipper
So what's your excuse for not building that robot idea you've been kicking around for months? Your excuse is invalid and we're here to explain why. In this day in age 'robots' are in every corner of our lives. So why are you not hacking them? It's time you take your computer skills and apply them to things that interact with the physical world. We will show you how easy it is to get started building your own robots to do your bidding or at a minimum make cool robot noises and impress the ladies*.

We will cover the various pitfalls we've run across building and operating various robots from advanced underwater gliders, beer delivery carts, CNC routers and 3D printers.

*Success with the ladies not guaranteed.

DECRYPTING DEF CON: FOUNDATIONS BEHIND SOME OF THE GAMES HACKERS PLAY

LosT
Continuing on his 101 talk from last year (building a foundational knowledge, or at least where to start doing so), LostboY will discuss the crypto, puzzles, and tech that is seen all over DEF CON each year. The floors, signs, program, lanyards, badges all have elements of mystery to them each year, and LosT will discuss the foundational knowledge/skills that were requisite in years past. The 4-bit processor that was drawn out on the floors last year will be discussed as a foundation on understanding how a processor works. (Everyone says they know a processor uses binary, but how many actually *know* what that means, or how to build one?) Fundamentals of digital logic design seem like a good next step from last year's talk. LosT will likely wax philosophical at some point as well.

INTRO TO WEB APPLICATION HACKING

Terrence "Tina" Gareau
This talk will will cover web application attack basics to get any n00b started on the path of web app pentesting. Specifically we will cover cross site scripting attacks in javascript, sql injections with a mysql backend, and remote/local file inclusions within PHP. Others people that may join us through the presentation will be Alex Heid, Rod Soto, p33p33, chatters, and a few other special friends of the fish.

OIL & GAS INFOSEC 101

AlxRogan
Ever wonder what it's like to secure off-shore platforms, field operations, and aging SCADA systems? Take a ride through how Oil & Gas companies operate and what the pitfalls are in trying to fix technology that predates enterprise IT and make them more secure. SCADA, wifi/radio/satellite communication, and corporate IT all come together and it's up to YOU to figure out how to make sense of it all.

WIRELESS PENETRATION TESTING 101 & WIRELESS CONTESTING

DaKahuna, RMellendick
Whether it's war-driving or doing penetration testing of wireless networks there are tools, hardware and software, that have shown to stand the test of time.

Some of the biggest difficulties that users encounter are hardware related. This talk will cover the hardware and software that we as experienced wireless pentesters recommend for users just starting out. To provide some hands on experience with wireless penetration testing, we have developed a number of mini-contest that will be conducted in the Wireless Village. We will provide an over view of these contest designed to test your wireless skills whether you are new to wireless or an experienced wireless penetration tester.

PENTESTER'S TOOLKIT

Anch
You've been hired to perform a penetration test, you have one week to prepare. What goes in the bag? What is worth lugging through airport security and what do you leave home. I'll go through my assessment bag and show you what I think is important and not, talk about tools and livecd's, what comes in handy and what I've cut out of my normal pen-test rig.

MEET PENTOO, THE LONGEST RUNNING PEN-TESTING LINUX DISTRO

ZeroChaos
Lead Developer, Pentoo Linux
You've been hired to perform a penetration test, you have one week to prepare. What goes in the bag? What is worth lugging through airport security and what do you leave home. I'll go through my assessment bag and show you what I think is important and not, talk about tools and livecd's, what comes in handy and what I've cut out of my normal pen-test rig.

THE ACLU PRESENTS: NSA SURVEILLANCE AND MORE

Alex Abdo
Staff Attorney, ACLU National Security Project
Catherine Crump
Staff Attorney, ACLU Speech Privacy & Technology Project
Christopher Soghoian
Principal Technologist, ACLU Speech Privacy and Technology Project
HaDe Crockford
ACLU of MA Technology for Liberty Project
Nicole Ozer
Technology and Civil Liberties Policy Director, ACLU of California
From the NSA's PRISM and metadata programs to IMSI catchers, location tracking to surveillance drones, and warrantless wiretapping to the AP's emails – this has been the year of surveillance. Come join the American Civil Liberties Union as we unravel the thicket of new technologies and laws that allow the U.S. government to surveil Americans in more intrusive ways than ever before. We will explore the latest news and trends in surveillance, reasons to despair, grounds to be hopeful, and ways in which you can help the ACLU's fight against government overreaching.

BUSINESS LOGIC FLAWS IN MOBILE OPERATORS SERVICES

Bogdan Alecu
Independent Security Researcher
GSM has been attacked in many different ways in the past years. But regardless of the protocol issues, there are also flaws in the logic of the mobile operators' services. One may think that finding an issue which affects only one specific operator in some country couldn't affect other operators. However, this is not the case as most of the operators are using the same equipment and have the same implementation of their services in all of the countries as the operator's group prefers to have a uniform service.

FEAR THE EVIL FOCA: IPV6 ATTACKS IN INTERNET CONNECTIONS

Chema Alonso
SECURITY RESEARCHER, INFORMATICA64
Windows boxes are running IPv6 by default so LANs are too. Internet is not yet ready for IPv6 worldwide, but... you can connect internal IPv6 networks to external IPv4 web sites with few packets. In this session you will see how using the new Evil FOCA tool, created to perform IPv6 networks attacks, it is possible to hack Internet IPv4 connections creating a man in the middle in IPv6 networks. And yes, it is only one point and click tool that does all for you. Evil FOCA does man in the middle IPv4, man in the middle IPv6, man in the middle IP4-IPv6, SSL strip, collects passwords, session cookies, and much more tricks. You will love this new Evil FOCA.

SUICIDE RISK ASSESSMENT AND INTERVENTION TACTICS

Amber Baldet
Investment Banking Technology
Suicide is the 10th leading cause of death in the United States, yet it persists as one of the few remaining taboo topics in modern society. Many characteristics linked to elevated suicide risk are prevalent in the technical community, and the effects of suicide within any community extend far beyond those directly involved. Prevention and intervention, however, are not a mystery. This workshop presents evidence based practices to assess suicide risk in others, and an introduction to the step-by-step practice of crisis intervention.

Rather than presenting a "depressing discussion of depression," attendees will learn the same threat modeling and crisis response best practices taught to first responders and mental health professionals, in a condensed format that answers many common questions people may be afraid to ask. Special attention will be paid to risk as it affects our particular community, and an overview of crisis network technical implementations / limitations (effects of digital anonymity & ethical concerns, etc.) will be presented.

Much like simple CPR training equips everyday people with the knowledge and confidence to help a heart attack victim that is likely a stranger, widespread dissemination of crisis intervention training aims to equip everyday people to prevent a suicide - most often, of a friend.

COMBATTING MAC OSX/IOS MALWARE WITH DATA VISUALIZATION

Remy Baumgarten
Security Engineer, ANRC-Services
Apple has successfully pushed both its mobile and desktop platforms into our homes, schools and work environments. With such a dominant push of its products into our everyday lives it comes as no surprise that both of Apple's operating systems, OSX and iOS should fall under attack by malware developers and network intruders. Numerous organizations and Enterprises who have implemented BYOD (bring your own device) company policies have seemingly neglected the security effort involved in protecting the network infrastructure from these potential insider threats. The complexity of analyzing Mach-O (Mach object file format) binaries and the rising prevalence of Mac-specific malware has created a real need for a new type of tool to assist in the analytic efforts required to rapidly identify malicious content. In this paper we will introduce Mach-O Viz, a Mach-O Interactive Data Visualization tool that lends itself to the role of aiding security engineers in quickly and efficiently identifying potentially malicious Mach-O files on the network, desktop and mobile devices of connected users.

MITM ALL THE IPV6 THINGS

Scott Behrens
Senior Security Consultant, Neohapsis
Brent Bandelgar
Associate Security Consultant, Neohapsis
Back in 2011, Alec Waters demonstrated how to overlay a malicious IPv6 network on top of an IPv4-only network, so that an attacker can carry out man-in-the-middle attacks on IPv4 traffic and subvert the assumed end to end security model. This attack is potentially powerful but requires involves a complex series of manual system configuration and setup activities, including the use of experimental and since-deprecated techniques. In addition, technology updates rendered Waters' implementation of the attack ineffective on certain platforms, such as Windows 8.

We reviewed the attack and tried it against current operating systems. We found configuration updates were needed to make it work against Windows 8 hosts and have packaged our setup into a script called "Sudden Six" to make launching the attack quick and painless. This attack now works against a variety of different platforms and operating systems, which will allow you to man-in-the-middle IPv6 traffic in record time.

This talk will discuss how the attack works as well as discuss our automation strategy and some pitfalls we uncovered. The "Sudden Six" configuration utility will be released and a demonstration of the attack against Windows 8 will be provided.

THE POLICY WONK LOUNGE

Sameer Bhalotra
Former White House Senior Director For Cybersecurity
Robert Brese
Chief Information Officer, Us Department Of Energy
Lt. General Robert Elder
Former Commander of 8Th Air Force And U.S. Strategic Command's Global Strike Component
Bruce Mcconnell
Deputy Undersecretaryfor Cybersecurity, Us Dept. Of Homeland Security
Mark Weatherford
Dept. Of Homeland Security's First Deputy Under Secretary for Cybersecurity
Professor James R. Lint
Retired Army Counterintelligence Special Agent
Can wonks hack it at DEF CON? Lean back and settle in for a stimulating evening of debate on Washington's most complex cybersecurity policy issues.

Join US Government insiders for an exclusive discussion session on domestic surveillance law, foreign computer criminals, law enforcement and criminal penalties, power grid regulation, user identity and privacy, and more. The debate rages in DC... and at DEF CON for one night only!

POWERPWNING: POST-EXPLOITING BY OVERPOWERING POWERSHELL

Joe Bialek
Security Engineer, Microsoft
PowerShell is a scripting language included with all modern Windows operating systems, which, among other features, provides access to the Win32 API and the capability to run scripts on remote servers without writing to disk. PowerShell scripts bypass application white listing, application-signing requirements, and generally bypass anti-virus as well.

While all of these characteristics are very desirable to a penetration tester, rewriting penetration test tools in PowerShell would be time consuming. Instead, I will show how to combine PowerShell and assembly to reflectively load existing EXE's and DLL's without writing to disk, triggering anti-virus, or triggering application whitelisting. I'll finish with several demonstrations of the Invoke-ReflectivePEInjection script in action.

PRESENTATIONS

TRANSCENDING CLOUD LIMITATIONS BY OBTAINING INNER PIECE

ZaK Blacher
Vulnerability & Malware Research Labs, Qualys

With the abundance of cloud storage providers competing for your data, some have taken to offering services in addition to free storage. This presentation demonstrates the ability to gain unlimited cloud storage by abusing an overlooked feature of some of these services.

MADE OPEN: HACKING CAPITALISM

Todd Bonnewell
Man With a Message, Madeopen.com

The game is Capitalism. The rule makers are the banks, corporations and governments. This presentation is about playing a game that is rigged by the rule makers, and winning in such fashion that the game is never the same. If you like breaking things and building them back up, or are a person, please at least watch this at a later time. I forgive you for not attending, but you will not forgive yourself for missing it.

DATA EVAPORATION FROM SSDS

Sam Bowne
Instructor, City College San Francisco

Files on magnetic hard drives remain on the drive even after they are deleted, so they can be recovered later with forensic tools. Sometimes SSDs work the same way, but under other conditions they erase this latent data in a "garbage collection" process. Understanding when and how this happens is important to forensic investigators and people who handle confidential data.

I'll explain the purpose of garbage collection, and how it is affected by the operating system, SSD model, BIOS settings, TRIM, and drive format. I'll demonstrate SSD data evaporation on a MacBook Air and a Windows system, using my "evap" tool (available for everyone to use) that makes it easy to test SSDs for data evaporation.

EVIL DOS ATTACKS AND STRONG DEFENSES

Sam Bowne, Matthew Prince

On the attack side, this talk will explain and demonstrate attacks which crash Mac OS X, Windows 8, Windows Server 2012, and Web servers; causing a BSOD or complete system freeze. The Mac and Windows systems fall to the new IPv6 Router Advertisement flood in thc-ipv6-2.1, but only after creating a vulnerable state with some "priming" router advertisements. Servers fail from Sockstress--a brutal TCP attack which was invented in 2008, but still remains effective today.

On the defense side: the inside story of the DDoS that almost Broke the Internet.

In March 2013, attackers launched an attack against Spamhaus that topped 300Gbps. Spamhaus gave us permission to talk about the details of the attack. While CloudFlare was able to fend off the attack, it exposed some vulnerabilities in the Internet's infrastructure that attackers will inevitably exploit. If an Internet-crippling attack happens, this is what it will look like. And here's what the network needs to do in order to protect itself.

RFID HACKING: LIVE FREE OR RFID HARD

Francis Brown
Managing Partner – Bishop Fox

Have you ever attended an RFID hacking presentation and walked away with more questions than answers? This talk will finally provide practical guidance on how RFID proximity badge systems work. We'll cover what you'll need to build out your own RFID physical penetration toolkit, and how to easily use an Arduino microcontroller to weaponize commercial RFID badge readers — turning them into custom, long-range RFID hacking tools.

This presentation will NOT weigh you down with theoretical details, discussions of radio frequencies and modulation schemes, or talk of inductive coupling. It WILL serve as a practical guide for penetration testers to understand the attack tools and techniques available to them for stealing and using RFID proximity badge information to gain unauthorized access to buildings and other secure areas. Schematics and Arduino code will be released, and 100 lucky audience members will receive a custom PCB they can insert into almost any commercial RFID reader to steal badge info and conveniently save it to a text file on a microSD card for later use (such as badge cloning). This solution will allow you to read cards from up to 3 feet away, a significant improvement over the few centimeter range of common RFID hacking tools.

OTP. IT WON'T SAVE YOU FROM FREE RIDES!

Bughardy, Eagle1753

RFID technologies are becoming more and more prevalent in our lives. This motivated us to study them, and in particular to study the MIFARE ULTRALIGHT chips, which are widely used in public/mass transport systems. We focused on multiple-ride tickets, and were surprised that MIFARE ULTRALIGHT chips do not seem to use any type of encryption. We were excited at the idea of simply cloning a new, unused ticket onto older ones to "refill" them. Our excitement was cut short by a security feature called OTP. OTP, in the context of MIFARE chips, is a sector of the data that can be edited (initialized) only one time. In this way, the ticket can store how many rides you still have, and this value cannot be changed back.

After much tinkering, we were able to completely bypass this security feature, by (ab)using a separate security feature, the so-called "lockbyte sector". Join us in this session to learn how we found out how to use security features of the chip against each other, and obtain endless free rides with a 5-ride ticket.

OPEN PUBLIC SENSORS, TREND MONITORING AND DATA FUSION

Daniel Burroughs
Associate Director of Technology, Center for Law Enforcement Technology, Training And Research

Our world is instrumented with countless sensors. While many are outside of our direct control, there is an incredible amount of publicly available information being generated and gathered all the time. While much of this data goes by unnoticed or ignored it contains fascinating insight into the behavior and trends that we see throughout society. The trick is being able to identify and isolate the useful patterns in this data and separate it from all the noise.

Previously, we looked at using sites such as Craigslist to provide a wealth of wonderfully categorized information and then used that to answer questions such as "What job categories are trending upward?", "What cities show the most (or the least) promise for technology careers?", and "What relationship is there between the number of bikes for sale and the number of prostitution ads?" After achieving initial success looking at a single source of data, the challenge becomes to generate more meaningful results by combining separate data sources that each views the world in a different way. Now we look across multiple, disparate sources of such data and attempt to build models based on the trends and relationships found therein.

CONDUCTING MASSIVE ATTACKS WITH OPEN SOURCE DISTRIBUTED COMPUTING

Alejandro Caceres
Owner, Hyperion Gray, LLC

Distributed computing is sexy. Don't believe us? In this talk we'll show you, on a deep, practical level and with lots of (mostly Python) code, how a highly automated and effective computer network attack could be crafted and enhanced with the help of distributed computing over 'Big Data' technologies. Our goal is to demystify the concept of using distributed computing for network attacks over an open source distributed computing cluster (Hadoop). By the end of this highly demo-focused talk you'll have an understanding of how an attacker could use three of our open source custom-written distributed computing attack tools, or easily build their own, to do whatever it is that they're into (we don't judge).

OFFENSIVE FORENSICS: CSI FOR THE BAD GUY

Benjamin Caudill
Principal Consultant, Rhino Security Labs

As a pentester, when was the last time you 'recovered' deleted files from the MFT of a pwned box? Ever used an index.dat parser for identifying your next target? Do you download a victim's hiberfil.sys whenever you can?

Despite the sensitive information uncovered through forensic techniques, the usage of such concepts have primarily been limited to investigations and incident response. In this talk, we will cover the basics of "Offensive Forensics", what information to look for, how to find it, and the use of old tools in a new way. After looking at the post-exploitation potential, we'll dive into real-world examples and release the first ever "Vulnerable [Forensics] by Design" machine!

UTILIZING POPULAR WEBSITES FOR MALICIOUS PURPOSES USING RDI

Daniel Chechik
Security Researcher, Trustwave Spiderlabs
Anat (Fox) Davidi
Security Researcher, Trustwave Spiderlabs

Reflected DOM Injection is a new attack vector that will be unveiled for the first time in our talk! We will explain the technique and show a live demo where we use it to hide malicious code within popular and trusted websites.

ABUSING NOSQL DATABASES

Ming Chow
Lecturer, Tufts University Department of Computer Science

The days of selecting from a few SQL database options for an application are over. There is now a plethora of NoSQL database options to choose from: some are better than others for certain jobs. There are good reasons why developers are choosing them over traditional SQL databases including performance, scalabiltiy, and ease-of-use. Unfortunately like for many hot techologies, security is largely an afterthought in NoSQL databases. This short but concise presentation will illustrate how poor the quality of security in many NoSQL database systems is. This presentation will not be confined to one particular NoSQL database system. Two sets of security issues will be discussed: those that affect all NoSQL database systems such as defaults, authentication, encryption; and those that affect specific NoSQL database systems such as MongoDB and CouchDB. The ideas that we now have a complicated heterogeneous problem and that defense-in-depth is even more necessary will be stressed. There is a common misconception that SQL injection attacks are eliminated by using a NoSQL database system. While specifically SQL injection is largely eliminated, injection attack vectors have increased thanks to JavaScript and the flexibility of NoSQL databases. This presentation will present and demo new classes of injection attacks. Attendees should be familiar with JavaScript and JSON.

LEGAL ASPECTS OF FULL SPECTRUM COMPUTER NETWORK (ACTIVE) DEFENSE

Robert Clark
Attorney

Full spectrum computer network (active) defense mean more than simply "hacking back". We've seen a lot of this issue lately. Orin Kerr and Stewart Baker had a lengthy debate about it online. New companies with some high visibility players claim they are providing "active defense" services to their clients. But all-in-all, what does this really mean? And why is it that when you go to your attorneys, they say a flat out, "No".

This presentation examines the entire legal regime surrounding full spectrum computer network (active) defense. It delves into those areas that are easily legal and looks at the controversial issues surrounding others. As such we will discuss technology and sensors (ECPA and the service provider exception); information control and management (DRM); and, "active defense" focusing on honeypot, beacons, deception (say hello to my little friend the Security and Exchange Commission); open source business intelligence gathering (CFAA, economic espionage; theft of trade secrets); trace back and retrieval of stolen data (CFAA).

Past presentations have shown much of what is taken away is audience driven in response to their questions and the subsequent discussion. And, as always, I try to impress upon computer security professionals the importance of working closely with their legal counsel early and often, and of course "Clark's Law" - explain the technical aspects of computer security to your attorneys at a third grade level so they can understand it and then turn around and explain it to a judge or jury at a first grade level.

BLUCAT: NETCAT FOR BLUETOOTH

Joseph Paul Cohen

TCP/IP has tools such as nmap and netcat to explore devices and create socket connections. Bluetooth has sockets but doesn't have the same tools. Blucat fills this need for the Bluetooth realm. Blucat can be thought of as a:

- debugging tool for bluetooth applications
- device exploration tool
- a component in building other applications

Blucat is designed to run on many different platforms (including Raspberry Pi) by abstracting core logic from native code using the Bluecove library to interact with a variety of Bluetooth stacks. This talk will go over the objectives, designs, and current results of the project. More information is at http://blucat.sourceforge.net/ .

HOME INVASION 2.0 - ATTACKING NETWORK-CONTROLLED CONSUMER DEVICES

Daniel "Unicornfurnace" Crowley
Managing Consultant, Spiderlabs, Trustwave
Jennifer "Savagejen" Savage
Software Engineer
David "Videoman" Bryan

A growing trend in electronics is to have them integrate with your home network in order to provide potentially useful features like automatic updates or to extend the usefulness of existing technologies such as door locks you can open and close from anywhere in the world. What this means for us as security professionals or even just as people living in a world of network-connected devices is that being compromised poses greater risk than before.

Once upon a time, a compromise only meant your data was out of your control. Today, it can enable control over the physical world resulting in discomfort, covert audio/video surveillance, physical access or even personal harm. If your door lock or space heater are compromised, you're going to have a very bad day. This talk will discuss the potential risks posed by network-attached devices and even demonstrate new attacks against products on the market today.

STEPPING P3WNS: ADVENTURES IN FULL SPECTRUM EMBEDDED EXPLOITATION (AND DEFENSE!)

Ang Cui
Ph.D Candidate, Columbia University
Michael Costello
Research Staff, Columbia UNiversity

Our presentation focuses on two live demonstrations of exploitation and defense of a wide array of ubiquitous networked embedded devices like printers, phones and routers.

The first demonstration will feature a proof-of-concept embedded worm capable of stealthy, autonomous polyspecies propagation. This PoC worm will feature at least one 0-day vulnerability on Cisco IP phones as well as several embedded device vulnerabilities previously disclosed by the authors. We will demonstrate how an attacker can gain stealthy and persistent access to the victim network via multiple remote initial attack vectors against routers and printers. Once inside, we will show how the attacker can use other embedded devices as stepping stones to compromise significant portions of the victim network without ever needing to compromise the general purpose computers residing on the network. Our PoC worm is capable of network reconnaissance, manual full-mesh propagation between IP phones, network printers and common networking equipment. Finally, we will demonstrate fully autonomous reconnaissance and exploitation of all embedded devices on the demo network.

PRESENTATIONS

The second demonstration showcases host-based embedded defense techniques, called Symbiotes, developed by the authors at Columbia University under support from DARPA's Cyber Fast Track and CRASH programs, as well as IARPA's STONESOUP and DHS's S&T Research programs.

The Symbiote is an OS and vendor agnostic host-based defense designed specifically for proprietary embedded systems. We will demonstrate the automated injection of Software Symbiotes into each vulnerable embedded device presented during the first demonstration. We then repeat all attack scenarios presented in the first demo against Symbiote defended devices to demonstrate real-time detection, alerting and mitigation of all malicious embedded implants used by our PoC worm. Lastly, we demonstrate the scalability and integration of Symbiote detection and alerting mechanisms into existing enterprise endpoint protection systems like Symantec End Point.

DO-IT-YOURSELF CELLULAR IDS

Sherri Davidoff
LMG Security
Scott Tretheim
LMG Security
David Harrison
LMG Security
Randi Price
LMG Security

For less than $500, you can build your own cellular intrusion detection system to detect malicious activity through your own local femtocell. Our team will show how we leveraged root access on a femtocell, reverse engineered the activation process, and turned it into a proof-of-concept cellular network intrusion monitoring system.

We leveraged commercial Home Node-Bs (""femtocells"") to create a 3G cellular network sniffer without needing to reimplement the UMTS or CDMA2000 protocol stacks. Inside a Faraday cage, we connected smartphones to modified femtocells running Linux distributions and redirected traffic to a Snort instance. Then we captured traffic from infected phones and showed how Snort was able to detect and alert upon malicious traffic. We also wrote our own CDMA protocol dissector in order to better analyze CDMA traffic.

The goal of this project was to develop a low-cost proof-of-concept method for capturing and analyzing cellular traffic using locally-deployed femtocells, which any security professional can build.

REVEALING EMBEDDED FINGERPRINTS: DERIVING INTELLIGENCE FROM USB STACK INTERACTIONS

Andy Davis
Research Director, NCC Group

Embedded systems are everywhere, from TVs to aircraft, printers to weapon control systems. As a security researcher when you are faced with one of these 'black boxes' to test, sometime in-situ, it is difficult to know where to start. However, if there is a USB port on the device there is useful information that can be gained. This talk is about using techniques to analyze USB stack interactions to provide information such as the OS running on the embedded device, the USB drivers installed and devices supported. The talk will also cover some of the more significant challenges faced by researchers attempting to exploit USB vulnerabilities using a Windows 8 USB bug recently discovered by the presenter (MSI3-027) as an example.

HOW TO DISCLOSE OR SELL AN EXPLOIT WITHOUT GETTING IN TROUBLE

James Denaro
Partner, Cipherlaw

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 20-minute session will cover the legal 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 being on the wrong end of civil and criminal legal action as a result of a publication or sale.

I CAN HEAR YOU NOW: TRAFFIC INTERCEPTION AND REMOTE MOBILE PHONE CLONING WITH A COMPROMISED CDMA FEMTOCELL

Doug DePerry
Senior Security Consultant, Isec Partners
Tom Ritter
Senior Security Consultant, Isec Partners

I have a box on my desk that your CDMA cell phone will automatically connect to while you send and receive phone calls, text messages, emails, and browse the Internet. I own this box. I watch all the traffic that crosses it and you don't even know you're connected to me. Welcome to the New World, where I, not them, own the towers. Oh, and thanks for giving me the box... for free.

This box is a femtocell, a low-power cellular base station given or sold to subscribers by mobile network operators. It works just like a small cell tower, using a home Internet connection to interface with the provider network. When in range, a mobile phone will connect to a femtocell as if it were a standard cell tower and send all its traffic through it without any indication to the user.

The state-of-the-art authentication protecting cell phone networks can be an imposing target. However, with the rising popularity of femtocells there is more than one way to attack a cellular network. Inside, they run Linux, and they can be hacked.

During this talk, we will demonstrate how we've used a femtocell for traffic interception of voice/SMS/data, active network attacks and explain how we were able to clone a mobile device without physical access.

PRIVACY IN DSRC CONNECTED VEHICLES

Christie Dudley
Privacy Legal Researcher

To date, remote vehicle communications such as OnStar have provided little in the way of privacy. The planned DSRC system will become the first large-scale nationwide direct public participation network outside of the internet. Much information and misinformation has been spread on what the upcoming DSRC system is and can do, especially in the information security community. The recent field trial in the US of a connected vehicle infrastructure raises the level of concern amongst all who are aware of existing privacy issues.

In this talk I will examine the current system high level design for North American vehicles, as set by international standards and used in a recent road test in Ann Arbor, Michigan, USA. I will consider privacy concerns for each portion of the system, identifying how they may be addressed by current approaches or otherwise considered solutions. I conclude with a discussion of the strategic value in engaging the privacy community during development efforts and the potential community role in raising privacy as a competitive advantage.

PWN'ING YOU(R) CYBER OFFENDERS

Piotr Duszynski
Senior Security Consultant,
Trustwave, Spiderlabs

It is commonly believed that Offensive Defense is just a theory that is difficult to be used effectively in practice, but that is not entirely true...

During my talk along with a new service emulation technique, that will render your port scanning results useless and leave you with an arduous analysis, I will focus on practical (automated) exploitation of a hackers' offensive toolbox. A few interesting attack vectors against software taken from the Internet will be presented.

It turns out you can get pwn'ed even through your Nmap scripts if you are not careful enough.

FROM NUKES TO CYBER – ALTERNATIVE APPROACHES FOR PROACTIVE DEFENSE AND MISSION ASSURANCE

Lt. General Robert Elder
USAF (Retired)

In typical military operations, the advantage goes to the offense because the initiator controls the timing and is able to concentrate forces. A good defense is designed to undermine the advantage of the offense. Proactive defense approaches include: masking (obfuscation), maneuvering, and hardening of critical capabilities. The other alternative, which is often characterized as resiliency or mission assurance, is to employ methods which deny the objectives of the offense. The expertise resident in the hacker community can improve both proactive defense and mission assurance.

NOISE FLOOR: EXPLORING THE WORLD OF UNINTENTIONAL RADIO EMISSIONS

Melissa Elliott
Application Security Researcher, Veracode

If it's electronic, it makes noise. Not necessarily noise that you and I can hear, of course – unless you know how to tune in. The air around us is filled with bloops, bleeps, and bzzts of machines going about their business, betraying their existence through walls or even from across the street. The unintentional noise lurking among intentional signals can even reveal what the machine is currently doing when it thinks it's keeping that information to itself. Attacks exploiting electromagnetic radiation, such as TEMPEST, have long been known, but government-sized budgets are no longer needed to procure the radio equipment. USB television receiver dongles can be used as software-defined radios (SDR) that cost less than a slice of Raspberry Pi. The goal of this talk is to show you that anyone with twenty bucks and some curiosity can learn a great deal about your computers and other equipment without ever leaving a trace, and you shouldn't neglect this risk when managing your organization's security .

ELECTROMECHANICAL PIN CRACKING WITH ROBOTIC RECONFIGURABLE BUTTON BASHER (AND C3BO)

Justin Engler
Senior Security Engineer, Isec Partners
Paul Vines

Password and PIN systems are often encountered on mobile devices. A software approach to cracking these systems is often the simplest, but in some cases there may be no better option than to start pushing buttons. This talk will cover automated PIN cracking techniques using two new tools and discuss the practicality of these attacks against various PIN-secured systems.

Robotic Reconfigurable Button Basher (R2B2) is a ~$200 robot designed to manually brute force PINs or other passwords via manual entry. R2B2 can operate on touch screens or physical buttons. R2B2 can also handle more esoteric lockscreen types such as pattern tracing.

Capacitive Cartesian Coordinate Bruteforceing Overlay (C3BO) is a combination of electronics designed to electrically simulate touches on a capacitive touch screen device. C3BO has no moving parts and can work faster than R2B2 in some circumstances.

Both tools are built with open source software. Parts lists, detailed build instructions, and STL files for 3d printed parts will be available for download.

A lucky volunteer will get to have their PIN cracked live on stage!

GOOGLE TV OR: HOW I LEARNED TO STOP WORRYING AND EXPLOIT SECURE BOOT

Amir Etemadieh
Research Scientist At Accuvant Labs
CJ Heres
IT Consultant
Mike Baker
Co-Founder Openwrt
Hans Nielsen
Senior Security Consultant At Matasano

Google TV is intended to bring the Android operating system out of the mobile environment and into consumers' living rooms. Unfortunately, content providers began to block streaming access to popular content from the Google TV platform which hindered its reach. Furthermore, the first generation of Google TV hardware used an Intel powered x86 chipset that fractured Google TV from that of the traditional ARM based Android ecosystem, preventing most Android applications with native code from functioning properly.

In our previous presentation at DEFCON 20, we discussed exploits found in the first generation of Google TV hardware and software. This presentation will be geared towards the newly released second generation of devices which includes models from a wider variety of OEM's such as Asus, Sony, LG, Vizio, Hisense, and Netgear.

Our demonstration will include newly discovered and undisclosed hardware exploits, software exploits, and manufacturer mistakes as well as discuss in detail how to exploit the new Secure Boot environment on the Marvell chipset.

In order to bypass Secure Boot on the Google TV we will release two separate exploits which will allow users to run an unsigned bootloader on Google TV devices. One of which affects specific configurations of the Linux kernel that can also be used for priviledge escalation against a multitude of other embedded devices.

GITDIGGER: CREATING USEFUL WORDLISTS FROM PUBLIC GITHUB REPOSITORIES

Jaime Filson (Vik)
Rob Fuller (Mubix)

This presentation intends to cover the thought process and logistics behind building a better wordlist using github public repositories as its source. With an estimated 2,000,000 github projects to date, how would one store that amount of data? Would you even want or need to? After downloading approximately 500,000 repositories, storing 6TB on multiple usb drives; this will be a story of one computer, bandwidth, basic python and how a small idea quickly got out of hand.

10000 YEN INTO THE SEA

Flipper

The use of a pressure housing in an underwater vehicle can be difficult to implement without becoming a cost-center. Flipper will walk the audience through a new design for an Autonomous Underwater Glider which challenges assumptions about what is required or necessary to deploy sensors, transmitters, and payloads across long distances in the ocean. The speaker assumes no priory knowledge of subject matter & hopes the audience can help him to find new applications for this Open Source Hardware project.

DEFEATING SEANDROID

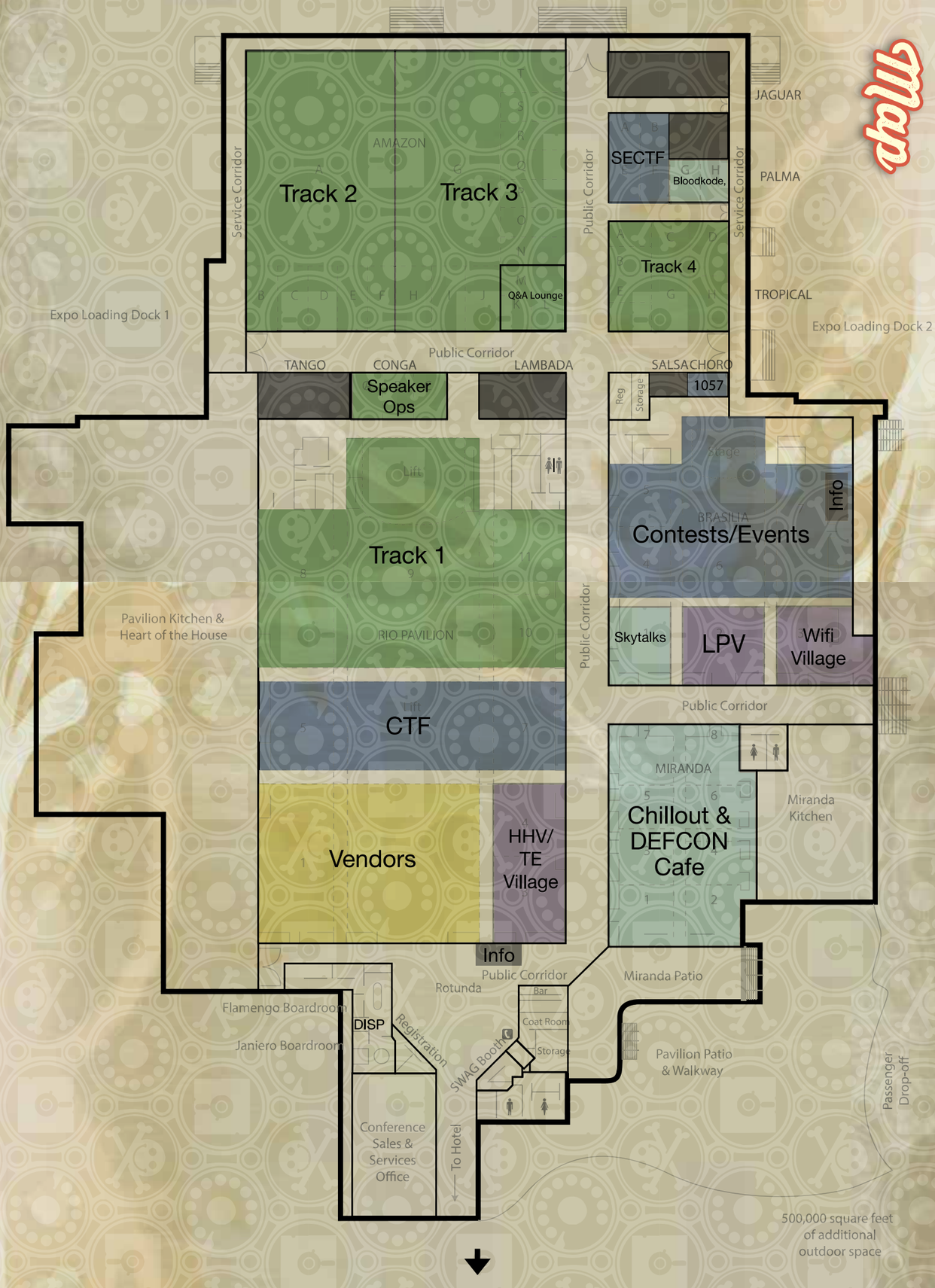
Pau Oliva Fora
Sr. Mobile Security Engineer, Viaforensics

Security Enhancements for Android (SEAndroid) enables the use of SELinux in Android in order to limit the damage that can be done by malicious apps, trying to make exploitation harder. Some OEMs are trying hard to implement extra mitigations in their devices, especially those aiming to reach the enterprise market. We will present some issues that are found in devices currently implementing SEAndroid, and demonstrate how vendors FAIL in properly implementing SEAndroid protection.

THE POLITICS OF PRIVACY AND TECHNOLOGY: FIGHTING AN UPHILL BATTLE

Eric Fulton
CEO, Subsector Solutions
Daniel Zolnikov
State Representative, Montana

In the past few decades the world has been dramatically transformed by technology. People have significantly evolved in how they interact with each other and the world; a side effect of this evolution is the drastic change in personal privacy. Private citizens, corporations, and governments all have different ideas on what privacy means and what information should be respected as private. Typically citizens don't realize their expectations of privacy are falsely held,


AMAZON
Track 2
Track 3
Service Corridor
Public Corridor
SECTF
Bloodkode,
JAGUAR
PALMA
Service Corridor
Track 4
Q&A Lounge
TROPICAL
Expo Loading Dock 1
Expo Loading Dock 2
Public Corridor
TANGO
CONGA
LAMBADA
SALSACHORO
Speaker Ops
1057
Reg
Storage
Stage
Lift
Info
BRASILIA
Contests/Events
Track 1
RIO PAVILION
Pavilion Kitchen & Heart of the House
Public Corridor
Skytalks
LPV
Wifi Village
Public Corridor
Lift
CTF
MIRANDA
Miranda Kitchen
Chillout & DEFCON Cafe
Vendors
HHV/ TE Village
Info
Public Corridor
Rotunda
Miranda Patio
Bar
Flamengo Boardroom
DISP
Registration
Coat Room
Janiero Boardroom
SWAG Booth
Storage
Pavilion Patio & Walkway
Passenger Drop-off
Conference Sales & Services Office
To Hotel
500,000 square feet of additional outdoor space

PRESENTATIONS

or more accurately that they have very little privacy left. Regarding privacy, decades have gone by without any action to protect an individual's privacy against entities buying, selling, storing, and using your private data. Policy can take years to enact, and the minimal legislative action happening leans toward protecting special interest groups who have great political sway.

Action needs to be taken. Policy needs to be created allowing businesses to operate while allowing individuals to keep their information private.
In the 2013 Montana Legislative Session Daniel Zolnikov, with the support of Eric Fulton, worked to introduce comprehensive legislation to protect the privacy of the citizens of Montana. Daniel Zolnikov and Eric Fulton will talk about the ideas behind the bill, the process of drafting and introducing legislation, presenting the bill before committee and the public testimony process, and the politics of why the bill ultimately died. The speakers will end the talk with lessons learned and thoughts on how to effectively pass future privacy legislation.

JAVA EVERY-DAYS: EXPLOITING SOFTWARE RUNNING ON 3 BILLION DEVICES

Brian Gorenc
Zero Day Initiative, Hp Security Research
Jasiel Spelman
Security Researcher

Over the last three years, Oracle Java has become the exploit author's best friend. And why not? Java has a rich attack surface, broad install base, and runs on multiple platforms allowing attackers to maximize their return-on-investment. The increased focus on uncovering weaknesses in the Java Runtime Environment (JRE) shifted research beyond classic memory corruption issues into abuses of the reflection API that allow for remote code execution. This talk focuses on the vulnerability trends in Java over the last three years and intersects public vulnerability data with Java vulnerabilities submitted to the Zero Day Initiative (ZDI) program.

We begin by reviewing Java's architecture and patch statistics to identify a set of vulnerable Java components. We then highlight the top five vulnerability types seen in ZDI researcher submissions that impact these JRE components and emphasize their recent historical significance. The presentation continues with an in-depth look at specific weaknesses in several Java sub-components, including vulnerability details and examples of how the vulnerabilities manifest and what vulnerability researchers should look for when auditing the component.

Finally, we discuss how attackers typically leverage weaknesses in Java. We focus on specific vulnerability types attackers and exploit kits authors are using and what they are doing beyond the vulnerability itself to compromise machines. We conclude with details on the vulnerabilities that were used in this year's Pwn2Own competition and review steps Oracle has taken to address recent issues uncovered in Java.

HARDWARE HACKING WITH MICROCONTROLLERS: A PANEL DISCUSSION

Joe Grand, Mark 'Smitty' Smith, LoST, Renderman, Firmwarez

Microcontrollers and embedded systems come in many shapes, sizes and flavors. From tiny 6-pin devices with only a few bytes of RAM (ala the DEF CON 14 Badge) to 32- bit, eight core multiprocessor systems (ala DEF CON 20 Badge), each has their own strengths and weaknesses. Engineers and designers tend to have their favorites, but how do they decide what part to work with? Join DEFCON Badge designers Joe Grand and LoSTBoY, master of embedded system design FirmWarez, devoted electronics hobbyist Smitty, and moderator extraordinaire RenderMan as they argue the virtues of their favorite microcontrollers and answer questions about hardware hacking. If you're just getting started with electronics and are trying to navigate the sea of available microcontrollers, microprocessors, and modules, this panel is for you.

JTAGULATOR: ASSISTED DISCOVERY OF ON-CHIP DEBUG INTERFACES

Joe Grand
aka Kingpin

On-chip debug (OCD) interfaces can provide chip-level control of a target device and are a primary vector used by hackers to extract program code or data, modify memory contents, or affect device operation on-the-fly. Depending on the complexity of the target device, manually locating available OCD connections can be a difficult and time consuming task, sometimes requiring physical destruction or modification of the device.

In this session, Joe will introduce the JTAGulator, an open source hardware tool that assists in identifying OCD connections from test points, vias, or components pads. He will discuss traditional hardware reverse engineering methods and prior art in this field, how OCD interfaces work, and how JTAGulator can simplify the task of discovering such interfaces.

PROTECTING DATA WITH SHORT-LIVED ENCRYPTION KEYS AND HARDWARE ROOT OF TRUST

Dan Griffin
President, JW Secure, Inc.

The US National Security Agency has been public about the inevitability of mobile computing and the need to support cloud-based service use for secret projects. General Alexander, head of the NSA, recently spoke of using smartphones as ID cards on classified networks.

And yet, mobile devices have a poor security track record, both as data repositories and as sources of trustworthy identity information. Cloud services are no better: current security features are oriented toward compliance and not toward real protection.

What if we could provide a strong link between mobile device identity, integrity, and the lifecycle of data retrieved from the cloud using only the hardware shipped with modern smartphones and tablets?

The good news is that we can do that with the trusted execution environment (TEE) features of the common system on a chip (SOC) mobile processor architectures using 'measurement-bound' encryption. This talk will describe how data can be encrypted to a specific device, how decryption is no longer possible when the device is compromised, and where the weaknesses are. I will demonstrate measurement-bound encryption in action. I will also announce the release of an open-source tool that implements it as well as a paper that describes the techniques for time-bound keys.

This is likely the very same way that NSA will be protecting the smartphones that will be used for classified information retrieval. Come learn how your government plans to keep its own secrets and how you can protect yours.

SO YOU THINK YOUR DOMAIN CONTROLLER IS SECURE?

Justin Hendricks
Security Engineer, Microsoft

Domain Controllers are the crown jewels of an organization. Once they fall, everything in the domain falls . Organizations go to great lengths to secure their domain controllers, however they often fail to properly secure the software used to manage these servers.

This presentation will cover unconventional methods for gaining domain admin by abusing commonly used management software that organizations deploy and use.

PHANTOM NETWORK SURVEILLANCE UAV / DRONE

Ricky Hill
Security Consultant

DARPA, 2011, sponsored a contest named UAVForge which challenged teams to build a prototype unmanned aerial vehicle (UAV). Mission: "UAV must be small enough to fit in a soldier's rucksack and able to fly to, perch & stare from useful locations for several hours near targets of interest to provide real-time (visual) persistent surveillance." Long story short: 140 teams participated, no one won. Crashes, remote piloting, & electronics problems all took their toll.

Flash forward to 2013 - Technology has improved significantly. Reading the UAVForge story, I was fascinated by the concept of "perch and stare" surveillance. I wondered if this technique could be extended from visual to wireless network discovery & exploitation?

Jan. 2013, DJI Innovations introduced a quadcopter known as the Phantom. Phantom quickly gained a reputation as the most stable platform for use in aerial photography and other, small electronics. Phantom uses a GPS autopilot and a "return to home" capability in case the flight goes wrong. So, I decided to become a proud Phantom owner. I built and now fly wireless missions using 2 payloads: [1] Wispy spectrum analyzers, and [2] an Internet-accessible WiFi Pineapple (Hak5).

In this presentation you will learn how to successfully outfit & fly a quadcopter equipped with tiny computers, plus utilize wireless survey & exploitation tools. Three missions will be covered: site survey, in-flight wifi discovery, plus extended roof-top wifi pineapple operation.

THE BLUETOOTH DEVICE DATABASE

Ryan Holeman
Senior Software Developer,
Ziften Technologies

As of 2013, it is estimated that there are now billions of bluetooth devices deployed worldwide. The goal of the Bluetooth Database Project is to track and freely distribute real time sightings and statistics of these wide spread devices. The data collected from these devices can be used to answer questions pertaining to various topics, such as device geolocation, device proliferation, population analysis, device misconfigurations, and an assortment of other security related analytics.

During this presentation I will go over the current community driven, distributed, real time, client/server architecture of the project. I will show off some of analytics that can be leveraged from the projects data sets. Finally, I will be releasing various open source open source bluetooth scanning clients (Linux, iOS, OSX). These clients are easily installable across various operating systems and can be used to systematically contribute data to the project.

DUDE, WTF IN MY CAR?

Alberto Garcia Illera
Javier Vazquez Vidal

The ECU tuning market is weird. There is little help from people in it, and most of the equipment is expensive. Well, not anymore! After hacking some equipment worth thousands of dollars, a new toy was born. Seed/Key algos broken, RSA busted… We will learn all about Bosch EDC15 and EDC16 car ECUs. How they communicate, what protocols they use, their security and why it is worth hacking them. There will be a demonstration of a tool that does all of these, and costs less than $25 to build..

RESTING ON YOUR LAURELS WILL GET YOU PWNED: EFFECTIVELY CODE REVIEWING REST APPLICATIONS TO AVOID GETTING PWNED

Abraham Kang
Director of R&D, Samsung
Dinis Cruz

Public REST APIs have become mainstream. It is not just startups such as Facebook and twitter at the fore front of the REST revolution. Now, almost every company that wants to expose services or an application programming interfaces does it using a publicly exposed REST API. Although, many people have given talks about attacking REST APIs from a pen-tester's point of view –little discussion has occurred related to application layer vulnerabilities in REST APIs.

This talk gives code reviewers the skills they need to identify and understand REST vulnerabilities at the application code level. The findings are a result of reviewing production REST applications as well as researching popular REST frameworks.

TORTURING OPEN GOVERNMENT SYSTEMS FOR FUN, PROFIT AND TIME TRAVEL

Tom Keenan
Professor, University of Calgary

"I'm from the government and I'm here to help you" takes on a sinister new meaning as jurisdictions around the world stumble over each other to 'set the people's data free'. NYC boasts in subway ads that 'our apps are whiz kid certified' (i.e. third party) which of course translates to 'we didn't pay for them, and don't blame us if somebody got it wrong and the bus don't come.' This session reports on my (and other people's) research aimed at prying out data that you're probably not supposed to have from Open Government Systems around the world. For example, Philadelphia, PA cavalierly posted the past 7 years of political contribution receipts which contained the full names and personal addresses of thousands of people, some of whom probably didn't want that information to be out there in such a convenient form. The entire database was also trivially downloadable as a CSV file and analysis of it yielded some fascinating and unexpected information. Referring back to classic computer science and accounting principles like 'least privilege' and 'segregation of duties' the presentation will suggest some ways to have our Open Data cake without letting snoopy people eat it.

THE DIRTY SOUTH – GETTING JUSTIFIED WITH TECHNOLOGY

David Kennedy
Founder & Principal Security Consultant, Trustedsec
Nick Hitchcock
Senior Security Consultant, Trustedsec

It seems that every day there's a new NextGen firewall, whitelisting and blacklisting, DLP, or the latest technology thats suppose to stop us. But does it really stop "hackers"? Truth is, naw not really. In this talk we'll be showing off the latest bypass techniques for the "latest" hacker stoppers, using a universally whitelisted website as our middle man for a command and control, social engineering our way into some of the toughest companies, and showing off some techniques that work for us. This talk is about throwing misconceptions of protection and safety out the window, and going back the dirty south. Where thinking outside of the box is a requirement. We'll be releasing two new tools, one that makes meterpreter invisible over the network, and the other a shell that uses a popular third party as the command and control. A vulnerability scanner won't help you herrrrrrre.

THE SECRET LIFE OF SIM CARDS

Karl Koscher
Grad Student, University of Washington
Eric Butler

SIM cards can do more than just authenticate your phone with your carrier. Small apps can be installed and run directly on the SIM separate from and without knowledge of the phone OS. Although SIM Applications are common in many parts of the world, they are mostly unknown in the U.S. and the closed nature of the ecosystem makes it difficult for hobbyists to find information and experiment.

This talk, based on our experience building SIM apps for the Toorcamp GSM network, explains what (U)SIM Toolkit Applications are, how they work, and how to develop them. We will explain the various pieces of technology involved, including the Java Card standard, which lets you write smart card applications using a subset of Java, and the GlobalPlatform standard, which is used to load and manage applications on a card. We will also talk about how these applications can be silently loaded, updated, and interacted with remotely over-the-air.

DECAPPING CHIPS THE EASY HARD WAY

Adam "Major Malfunction" Laurie
Code Monkey, Aperture Labs
Zac Franken
Chip Monkey, Aperture Labs

For some time it has been possible to discover the inner workings of microprocessors with the help of a microscope and some nasty chemicals such as fuming nitric acid. However, unless you have access to a university or work science lab, this is beyond the reach of most hackers, and, even it were to be attempted, difficult and potentially extremely dangerous.

SKYTALKS

Skytalks is a track at Defcon presented by 303 for the Defcon community. Its purpose: for people to show the cutting edge in technology and research -- the kind you can't or don't want to do at home.

This is classic, old-school Defcon: no cameras, no recording. No pre-con content takedowns. No sobriety. No bullshit.

FRIDAY, AUG 2

9am **TBA**
10am **Antitree**
Bringing Intelligence back to the hacker community
11am **Ryan Linn**
Swiping Cards At The Source: POS & Cash Machine Security
12pm **Andrea Matwyshyn**
Hacked Up
1pm **Anch**
The Art of the Rig, Building a pen-test rig that isn't worthless
2pm **JP Dunning**
The Glitch: Bringing Hacking Hardware to the Masses
3pm **Kevin Carter**
Hacking Interfaces with your Mind
4pm **Mohamed Saher**
Project CANCER: Bringing VX Back
5pm **Alex Heid, Rod Soto, Tuna, Roamer**
Digital Warfare, InfoSec Research, and The 2nd Amendment (2 hrs)

SATURDAY, AUG 3

9am **Jimmy Shah, David Shaw, Matt McDevitt**
Discovering Dark Matter: Towards better Android Malware Heuristics
10am **JP Bourget & Bruce Potter**
Cycling and Hacking to Defcon
11am **Valerie Thomas, Harry Regan**
All Your Base Still Belong To Us: Physical Penetration Testing Tales From The Trenches
12pm **Jason NOObz, Raj**
#FreeCrypt0s: Using SDR to prevent him from getting rooted!
1pm **Chris Roberts**
Hacking the Brew
2pm **Panel - Oldtimers v. N00bz 2.0**
3pm **Rob Bird**
Occam's Katana: Defeating Big Data Analytics (2 hrs)
5pm **Alex Heid, James Ball, YTcracker, Travis Tolle, Chris Snyder**
Bitcoin, Litecoin, & Alternative Cryptocurrencies - Pros, Cons, & Threats (2 hrs)

SUNDAY, AUG 4

9am **TBA**
10am **TBA**
11am **AcrOnym, Johan Hybinette**
LAZZORS! PEW! PEW!
12pm **Christie Dudley**
Strange interactions in personal data: Brokers and the CFAA
1pm **Onlychick**
The Continued Rise of Idiocracy: CCSS, PBI and other education acronyms that nobody understands
2pm **James Costello**
Network Survival WCS
3pm **Tim Krabec**
Owning Management with Standards
4pm **TBA**
5pm **CLOSED - See you in 2014!**

Photo, Art: DanChick.com With Tashays, AcrOnym

SkyTalks is located in Brasilia 1. Schdule updates and changes on https://SkyTalks.info or Twitter @dcskytalks

PRESENTATIONS

In this talk we will go through our own adventures in tackling the issue from the point of view of the back-room hacker/researcher, and how we have solved many of the problems using only tools and devices that were freely and cheaply available from online sources such as Ebay.

There is also the secondary problem of what to do with the chip once you've decapped it. For example: if you've taken microscopic images of a masked ROM, in theory you can extract the code, but in practice you're looking at thousands of tiny dots, each of which represent a 0 or a 1, which, once correctly read and compiled into HEX, will represent the original byte code. Many projects (e.g. MAME) have used crowd-sourcing as a means of converting the images by eye, but we will present a software tool that semi-automates this process and we'll demonstrate how what was once the works of tens if not hundreds of hours can be reduced to a few minutes.

KEY DECODING AND DUPLICATION ATTACKS FOR THE SCHLAGE PRIMUS HIGH-SECURITY LOCK

David Lawrence
Student, Massachusetts Institute of Technology
Gabriel Harpman
Student, Massachusetts Institute of Technology
Robert Johnson
Student, Massachusetts Institute of Technology

The Schlage Primus is one of the most common high-security locks in the United States. We reverse-engineered the operation of this lock, constructed a parameterized 3d model of a working key, and constructed a software tool to produce such a 3d model given the code number for any key. We then used this tool to 3d print working Primus keys with a variety of 3d printing processes. In our talk, we will discuss the reverse-engineering process, demonstrate our software tool, examine the working 3d printed keys, and discuss the security ramifications of this process.

HOW TO USE CSP TO STOP XSS

Kenneth Lee
Product Security Engineer, Etsy Inc.

Crosssite scripting attacks have always been a mainstay of the OWASP Top 10 list. The problem with detecting XSS is that you can't go looking at web log traffic to determine if a request contains an actual crosssite scripting attack attempt, much less one that will actually succeed against your defenses. Our work has helped reveal some nuances with implementing content security policy to help detect and prevent XSS attacks across a major website. This talk will demonstrate a new python based tool that we are open sourcing for Defcon that combines client and serverbased whitelisting mechanisms to verify unauthorized scripts (I.e. XSS) running on a page, mixed content, and inline javascript across a site..

MEET THE VCS

Ping Li
Partner, Accel Partners
Matt Ocko
Partner, Data Collective
Phil Paul
Founder Of Paul Capital And Top Tier Capital
Eileen Burbidge
Partner, Passion Capital

Venture capital investments have reached the highest level since the dot-com days. Almost seven billion dollars was invested last quarter alone. While clean-tech deals hit a new low, security deals increased the most. Security is the new black. How should we spend the next billion? Meet the VCs and strategize on the future!

THIS PRESENTATION WILL SELF-DESTRUCT IN 45 MINUTES: A FORENSIC DEEP DIVE INTO SELF-DESTRUCTING MESSAGE APPS

Drea London
DIGITAL FORENSIC EXAMINER, STROZ FRIEDBERG
Kyle O'Meara
Digital Forensic Examiner, Stroz Friedberg

Prior to 2013, the phrase 'Self Destructing Message' was most commonly associated with Inspector Gadget, Maxwell Smart, and the occasional Tom Cruise movie. With the advent of smartphone apps like Snapchat, Wickr, and Facebook Poke, the self-destructing message has left the world of 'International Men of Mystery' and arrived to the civilian world by way of smart phone applications. These apps, and others, claim to provide ephemeral or private messaging to assure senders that their messages are burnt after reading.

A message can be encrypted, but that does not make it clandestine or deniable. Through the use of forensic images, packet captures, and API review - we have recovered a wide range of artifacts from messages before, after, and during transmission. We are neutral, fact finding, forensic examiners on a mission. A mission to seek truth and provide you with the results of our deep dive forensic review of self-destructing messaging smartphone apps.

HIVEMIND: DISTRIBUTED FILE STORAGE USING JAVASCRIPT BOTNETS

Sean Malone
Principal Security Consultant, Fusionx

Some data is too sensitive or volatile to store on systems you own. What if we could store it somewhere else without compromising the security or availability of the data, while leveraging intended functionality to do so? This presentation will cover the methodology and tools required to create a distributed file store built on top of a JavaScript botnet. This type of data storage offers redundancy, encryption, and plausible deniability, but still allows you to store a virtually unlimited amount of data in any type of file. They can seize your server – but the data's not there!

GOPRO OR GTFO: A TALE OF REVERSING AN EMBEDDED SYSTEM CONSTITUTION

Todd Manning
Senior Research Consultant, Accuvant Labs
Zach Lanier
Senior Research Consultant, Accuvant Labs

Embedded systems are shrinking in size and becoming widely used in many consumer devices. High quality optic sensors and lenses are also shrinking in size. The GoPro Hero 3 camera leverages high quality camera equipment with multiple embedded operating systems to offer not only great imagery, but an interesting platform to explore and understand.

We'll explore the hardware used in the device to handle imaging, networking, and other I/O. We will disect the camera software, giving the audience a look at how the camera functions. We will explain the multiple layers of software running on the device, and show attack surfaces exposed to attackers.

We will present ways to turn the GoPro into a remote audio/video bug. We'll present some interesting ways to interface existing software with the AV capabilities, and present a library to control the device remotely.

A THORNY PIECE OF MALWARE (AND ME): THE NASTINESS OF SEH, VFTABLES & MULTI-THREADING

Marion Marschalek
Analyst, Ikarus Security Software Gmbh

Reverse Engineering is the supreme discipline in analyzing malware, how else would you find out all capabilities of a malicious sample? But this task gets trickier nearly every day, as malware authors apply new techniques to evade analysis. Even worse, documentation of said techniques is barely existent, which makes our job even harder.

This talk will focus on the challenges of a specifically thorny piece of malware, detected as Backdoor.Win32.Banito. It will discuss the palette of anti-analysis measures found and show a path through a multi-threaded file-infecting spy bot. The talk will try to shed some light on the merely shallow documentation of the binary layout of Windows Structured Exception Handling (SEH), point out complications in analyzing object oriented C++ binaries and give an insight on how to tackle multi-threaded executables.

PRESENTATIONS

PWN THE PWN PLUG: ANALYZING AND COUNTER-ATTACKING ATTACKER-IMPLANTED DEVICES

Wesley McGrew
Research Associate, Mississippi State University

Malicious attackers and penetration testers alike are drawn to the ease and convenience of small, disguise-able attacker-controlled devices that can be implanted physically in a target organization. When such devices are discovered in an organization, that organization may wish to perform a forensic analysis of the device in order to determine what systems it has compromised, what information has been gathered, and any information that can help identify the attacker. Also, attacker-implanted penetration testing software and hardware may also be the target of counter-attack. Malicious attackers may compromise penetration testers' devices in order to surreptitiously gather information across multiple targets and pentests. The very tools we rely on to test security may provide an attractive attack surface for third parties.

In this talk, procedures for forensic examination and zero-day vulnerabilities that lead to remote compromise of the Pwn Plug will be discussed and demonstrated as a case study. Possible attack scenarios will be discussed.

GETTING THE GOODS WITH SMBEXEC

Eric Milam
Principal Consultant, Accuvant Labs

Individuals often upload and execute a payload to a remote system during penetration tests for foot printing, gathering information, and to compromise additional hosts. When trying to remain stealthy, uploading a shell to a target may not be wise. smbexec takes advantage of native Windows functionality and SMB authentication to execute commands on remote Windows systems without having to upload a payload, decreasing the likelihood of being stopped by AntiVirus.

The original intent of creating smbexec was to upload and execute obfuscated payloads using samba tools. Since the first PoC, it has expanded its capability to do more, including dumping local and domain cached password hashes, clear text passwords from memory, and stealing the NTDS.dit file from a Windows Domain controller all without the need for a shell on the victim.

We will explore the creation of smbexec, the components behind it, and how to leverage its functionality to get the goods from a system without having to use a payload.

ADVENTURES IN AUTOMOTIVE NETWORKS AND CONTROL UNITS

Charlie Miller
Security Engineer, Twitter
Chris Valasek
Director Of Security Intelligence, Ioactive, Inc.

Automotive computers, or Electronic Control Units (ECU), were originally introduced to help with fuel efficiency and emissions problems of the 1970s but evolved into integral parts of in-car entertainment, safety controls, and enhanced automotive functionality. This presentation will examine some controls in two modern automobiles from a security researcheris point of view. We will first cover the requisite tools and software needed to analyze a Controller Area Network (CAN) bus. Secondly, we will demo software to show how data can be read and written to the CAN bus. Then we will show how certain proprietary messages can be replayed by a device hooked up to an ODB-II connection to perform critical car functionality, such as braking and steering. Finally, weill discuss aspects of reading and modifying the firmware of ECUs installed in today's modern automobile.

POWERPRETER: POST EXPLOITATION LIKE A BOSS

Nikhil Mittal
Security Researcher

Powerpreter is "The" post exploitation tool. It is written completely in powershell which is present on all modern Windows systems. Powerpreter has multiple capabilties which any post exploitation shell worth its salt must have, minus the detection by anti virus or other countermeasure tools. Powerpreter has, to name a few, functions like stealing infromation, logging keys, dumping system secrets, in-memory code execution, getting user credenitals in plain, introducing vulnerabilties, stealing/modifying registry, web server and impersonate users. It is also capable of backdooring a target using multiple methods/payloads which could be controlled using top third party websites. Based on available privs, it could be used to pivot to other machines on a network and thus execute commands, code, powershell scripts etc. on those. It also contains a web shell which includes all these functionalities. It also has limited ability to clean up the system and tinker with logs. Almost all the capabilities of Powerpreter are persistent across reboots, memory resident and hard to detect. Powerpreter uses powershell which enables it not to use any "foreign" code. It could be deployed in a skeleton mode which pulls functionality from the internet on demand. It aims to improve Windows post exploitation practices and help in the most important phase of a Pen Test. The talk will be full of live demonstrations.

KILL 'EM ALL — DDOS PROTECTION TOTAL ANNIHILATION!

Tony Miu
Technical Director, Bloodspear Research Group
Wai-Leng Lee
VP of Engineering, Bloodspear Research Group

With the advent of paid DDoS protection in the forms of CleanPipe, CDN / Cloud or whatnot, the sitting ducks have stood up and donned armors... or so they think! We're here to rip apart this false sense of security by dissecting each and every mitigation techniques you can buy today, showing you in clinical details how exactly they work and how they can be defeated.

Essentially we developed a 3-fold attack methodology:

- stay just below red-flag rate threshold,
- mask our attack traffics inconspicuous,
- emulate the behavior of a real networking stack with a human operator behind it in order to spoof the correct response to challenges,
- ???
- PROFIT!

We will explain all the required look-innocent headers, TCP / HTTP challenge-response handshakes,JS auth bypass, etc. etc. in meticulous details. With that knowledge you too can be a DDoS ninja! Our PoC attack tool "Kill-em-All" will then be introduced as a platform to put what you've learned into practice, empowering you to bypass all DDoS mitigation layers and get straight through to the backend where havoc could be wrought. Oh and for the skeptics among you, we'll be showing testing results against specific products and services.

DEF CON COMEDY JAM PART VI. RETURN OF THE FAIL

David Mortman
Chief Security Architect, Enstratius
Rich Mogull
Analyst & Ceo, Securosis
Chris Hoff
Rational Security
Dave Maynor
Errata
Larry Pesce
Pauldotcom.com Enernex
James Arlen
Liquidmatrix/Leviathan Security
Rob Graham
Errata
Alex Rothman
Shostack, Esq.

You know you can't stay away! The most talked about panel at DEF CON! More FAIL than you can shake a stick at. Come hear some of the loudest mouths in the industry talk about the epic security failures of the last year. So much fail, you'll need waffles to make it through. Nothing is sacred not even each other. Over the last two years, we've raised over $2000 for the EFF, let's see how much we can raise this year.

PLEASE INSERT INJECT MORE COINS

Nicolas Oberli
Security Engineer, SCRT

The ccTalk protocol is widely used in the vending machine sector as well as casino gaming industry, but is actually not that much known, and very little information exists about it except the official documentation. This protocol is used to transfer money-related information between various devices and the machine mainboard like the value of the inserted bill or how many coins need to be given as change to the customer. This talk presents an introduction to the ccTalk protocol, its usage and various funny facts about it. Material presented will include a ccTalk server that can be used for DIY projects and various tools to help analyse and interact with a ccTalk bus.

STALKING A CITY FOR FUN AND FRIVOLITY

Brendan O'Connor

Tired of the government being the only entity around that can keep tabs on a whole city at once? Frustrated by dictators du jour knowing more about you than you know about them? Fed up with agents provocateur slipping into your protests, rallies, or golf outings?

Suffer no more, because CreepyDOL is here to help! With open-source software, off-the-shelf sensors, several layers of encryption, and a deployment methodology of "pull pin, point toward privacy insurance claimant," it allows anyone to track everyone in a neighborhood, suburb, or city from the comfort of their sofa. For just four easy hardware purchases of $131.95, you, too can move up from small-time weirding out to the big leagues of total information awareness: deploy CreepyDOL today!

ASK THE EFF: THE YEAR IN DIGITAL CIVIL LIBERTIES

Kurt Opsahl
Electronic Frontier Foundation
Macia Hoffmann
Fellow, EFF
Dan Auerbach
Staff Technologist, EFF
Eva Galperin
Global Policy Analyst, EFF
Marc Jaycox
Policy Analyst and Legislative Assistant, EFF
Mitch Stoltz
Staff Attorney, EFF

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.

FAST FORENSICS USING SIMPLE STATISTICS AND COOL TOOLS

John Ortiz
Computer Engineer, Crucial Security/Harris

Ever been attacked by malicious code leaving unknown files all over your computer? Trying to figure out if a file is encrypted or just compressed? Is the file really something else? Is there hidden data? Are you short on time! This talk leads you through file identification and analysis using some custom FREE tools that apply statistics and visualization to answer these questions and more. You can often identify files by their statistical picture and I am going to show you how.

We can find some hidden data (steganalysis), easily determine if an executable file is packed or obfuscated, find appended data, figure out if the file is really what it purports to be and even aid in reversing XOR encryption. The final proof of concept program allows you to statistically identify (i.e. no magic numbers or header information used) some file types autonomously for an entire hard drive. The Windows-based tools (mostly math so adaptable to Linux) and source code are free!

VOIP WARS: RETURN OF THE SIP

Fatih Ozavci
Information Security Researcher And Consultant, Viproy Security

NGN (Next Generation Network) is modern TDM/PSTN system for communication infrastructure. SIP (Session Initiation Protocol) Servers are center of NGN services, they provide signaling services. SIP based communication is insecure, because of protocol implementation. Based on this fact, NGN is not actually Next Generation. It can be hacked with old stuff, but a few new attack types will be demonstrated in this presentation.

This presentation includes that basic attack types for NGN infrastructure, old school techniques for SIP analysis, a new hacking tool to analysis of SIP services and SIP Trust Hacking technique. Also a few fuzzing techniques will be explained in this presentation.

SIP networks provide its services based on Trust Infrastructure. SIP Soft Switches trust each other and accept calls from trusted SIP servers. A new technique will be demonstrated in this presentation, Hacking Trust Relationships Between SIP Gateways. SIP trust will be detected and hacked with a sip trust analyzer tool. For explaining basic attack types, a few tools will be demonstrated such as footprinting, register, enumerator, bruteforcer, call analyzer and SIP proxy.

Another dangerous thing is outdated software in NGN infrastructure. VoIP devices have responsibilities to serve signaling such as MSAN, MGW and Soft Switches. They support SIP protocol with vulnerable software which should be analyzed. New fuzzing techniques such as Response based fuzzing, MITM fuzzing and proxy tool usage will be explained.

EXPLOITING MUSIC STREAMING WITH JAVASCRIPT

Franz Payer
Programmer, Tactical Network Solutions

As the music industry transitioned from physical to digital distribution, they have forgotten the one thing they hold most dear to them: Their DRM. Many browser-based music streaming services use no DRM to secure their music. By doing this, they leave their library of high quality songs free for the picking.

This presentation details the use of JavaScript to circumvent the security of several browser-based music streaming services. By reverse engineering the code for several music players, it is possible to mimic the music player to download songs rather than stream them. Many services that are too difficult or obfuscated to reverse engineer can still be exploited by intercepting streaming traffic and making identical requests to downloads songs. This presentation covers the basics of music streaming, demonstrates browser-based traffic logging to identify and download music files, and describes the use of JavaScript to mimic the legitimate player in order to bypass security. The end result is a Google-Chrome extension which will allow users to download songs as they stream them.

THE CAVALRY ISN'T COMING: STARTING THE REVOLUTION TO FSCK IT ALL!

Nicholas J. Percoco
SENIOR VICE PRESIDENT AND HEAD OF SPIDERLABS, TRUSTWAVE
Joshua Corman
DIRECTOR OF SECURITY INTELLIGENCE, AKAMAI TECHNOLOGIES

We have some good news and some bad news. The good news is that security is now top of mind for the people of planet Earth. The bad news is that their security illiteracy has lead to very dangerous precedents and this is likely just the beginning. The reactionary stances taken by the hacker community has induced burnout and fatigue with many of us watching our own demise. We're here to help us all hit rock bottom in the pursuit of something better. At some point the pain of maintaining inertia will exceed the pain of making changes, so it is time for some uncomfortable experimentation. While

PRESENTATIONS

it may be overwhelming to think about, this is what we do. We hack systems. Finding flaws in the digital world comes naturally to us. We can and must do the same to the physical world; the media, governments, and lawmakers in order to survive the next decade. Let's get started.

ACL STEGANOGRAPHY - PERMISSIONS TO HIDE YOUR PORN

MIchael PErklin
Security Researcher

Everyone's heard the claim: Security through obscurity is no security at all. Challenging this claim is the entire field of steganography itself - the art of hiding things in plain sight. Most people know you can hide a text file inside a photograph, or embed a photograph inside an MP3. But how does this work under the hood? What's new in the stego field?

This talk will explore how various techniques employed by older steganographic tools work and will discuss a new technique developed by the speaker which embodies both data hiding and data enciphering properties by encoding data inside NTFS volumes. A new tool will be released during this talk that will allow attendees to both encode and decode data with this new scheme.

DOING BAD THINGS TO `GOOD` SECURITY APPLIANCES

Phorkus (Mark Carey)
Chief SCientist, Peak Security
Evilrob (Rob Bathurst)
That Guy

The problem with security appliances is verifying that they are as good as the marketing has lead you to believe. You need to spend lots of money to buy a unit, or figure out how to obtain it another way; we chose eBay. We now have a hardened, encrypted, AES 256 tape storage unit and a mission, break it every way possible! We're going to dive into the finer points of the pain required to actually evaluate and disassemble a harden security appliance. We'll be delving into such fun topics as epoxy melting, de-soldering, ROM chip reading, FGPA configuration recreation, Verilog decoding, recovering the various key strands that keep the device/data secure, and any other topics we end up straying into.

LET'S SCREW WITH NMAP

Gregory Pickett
Penetration tester, Hellfire Security

Differences in packet headers allow tools like nmap to fingerprint operating systems. My new approach to packet normalization removes these header differences. Starting TTL, TCP Options used, and TCP Option order, after normalization, are the same from one packet to the next no matter which operating system sends it. If we normalized the packets transiting our network, could we keep nmap, and tools like it from remotely fingerprinting hosts? It turns out that we can, and we can for most hosts on our network.

The proof of concept that I developed (idguard) does just that. A Linux Kernel module, it will be installed as part of the embedded firmware of a Linux-based router, and placed on the local network. Idguard will then give all the packets flowing through the router the same starting TTL, the same selection of TCP options, and the same TCP option order, causing nmap to fail in its attempt to fingerprint hosts on the network.

In this session, we'll review packet normalization techniques and how they can be applied to the traffic flowing through our switches to make hosts that they support resistant to fingerprinting, even by nmap. We'll walk through the process from start to finish, from the selection and design of the transformations (some old, some new), to the development of the proof of concept, and finally to the demonstration of idguard itself on a RouterBoard model RB450 router. Followed up by a discussion of the issues involved, the challenges to overcome, and the obstacles to deploying this in a production environment.

DEFENDING NETWORKS WITH INCOMPLETE INFORMATION: A MACHINE LEARNING APPROACH

Alexandre Pinto
Security Researcher

Let's face it: we may win some battles, but we are losing the war pretty badly. Regardless of the advances in malware and targeted attacks detection technologies, our top security practitioners can only do so much in a 24 hour day. Even less, if you let them eat and sleep. On the other hand, there is a severe shortage of capable people to do "simple" security monitoring effectively, let alone complex incident detection and response.

Enter the use of Machine Learning as a way to automatically prioritize and classify potential events and attacks as something can could potentially be blocked automatically, is clearly benign, or is really worth the time of your analyst.

In this presentation we will present publicly for the first time an actual implementation of those concepts, in the form of a free-to-use web service. It leverages OSINT and knowledge about the spatial distribution of the Internet to generate a fluid and constantly updated classifier that pinpoints areas of interest on submitted network traffic logs.

WE ARE LEGION: PENTESTING WITH AN ARMY OF LOW-POWER LOW-COST DEVICES

Dr. Philip Polstra
Hacker in Residence, University of Dubuque

This talk will show attendees how they can do penetration testing with a network of small, battery-powered, penetration testing systems. The small devices discussed will be running a version of The Deck, a full-featured penetration testing and forensics Linux distro. The Deck runs on the BeagleBoard and BeagleBone family of devices (including the next-gen BeagleBone released in April aka the Raspberry Pi killer). These devices are easily hidden and can run for days to weeks off of battery power thanks to their low power consumption. Various configurations will be presented including a device the size of a deck of cards that is easily attached to the back of a computer which is powered by USB and can be connected inline with the computer's Ethernet connection. While each device running The Deck is a full-featured penetration testing platform, connecting systems together via 802.15.4 networking allows even more power and flexibility. Devices may be constructed for $70-$200 each depending on configuration with the typical device costing less than $100. Devices may be located up to 1 mile from each other and from the command console which could also be running The Deck or any other version of Linux. A powerful pentesting army is easily built for much less than the cost of an Apple MacBook Pro.

THE ROAD LESS SURREPTITIOUSLY TRAVELED

pukingmonkey

Anonymously driving your own vehicle is becoming unattainable with the proliferation of automatic license plate readers (ALPRs) now coming into wide-spread use. Combined with always-on electronic toll tags, smart phone traffic apps and even plain cell phones are adding to this problem. There is little public disclosure of this tracking and little legislation limiting the length of time data is retained, even if it is not involved in any investigation. History, laws, funding, detection, and their technological limitations, will be explored in this talk.

HACKER LAW SCHOOL

Jim Rennie
Attorney
Marcia Hoffmann
Attorney

In the past year, several high-profile prosecutions of hackers have underscored the need for legal education in our community. This workshop will provide you with the fundamentals of Intellectual Property, Crimimal Law, and Criminal Procedure that you need to protect yourself. Learn where the grey areas of law are that increase your risk. This session will also enable you to better understand the deeper in-depth legal talks provided on the other days of DefCon. Hacker Law School -- We Went to Law School so You Don't Have to.

DEFENSE BY NUMBERS: MAKING PROBLEMS FOR SCRIPT KIDDIES AND SCANNER MONKEYS

Chris John Riley

On the surface most common browsers look the same, function the same, and deliver web content to the user in a relatively uniformed fashion. Under the shiny surface however, the way specific user agents handle traffic varies in a number of interesting and unique ways. This variation allows for defenders to play games with attackers and scripted attacks in a way that most normal users will never even see.

This talk will attempt to show that differences in how different user agents handle web server responses (specifically status codes) can be used to improve the defensive posture of modern web applications while causing headaches for the average script kiddy or scanner monkey!

DE-ANONYMIZING ALT.ANONYMOUS.MESSAGES

Tom Ritter

This is a retrospective of computer security research and the process of building a secure operating system for the US government 1983-1990. The paper presents the case study of Kernelized Secure Operating System (KSOS), an AI security-kernel operating system. KSOS was written to protect SCI/compartmented data (sometimes referred to as "above TOP SECRET"), and entered pr.

NETWORK ANTI-RECONNAISSANCE: MESSING WITH NMAP THROUGH SMOKE AND MIRRORS

Dan 'Alff4' Petro
Security Researcher, Datasoft Corp.

In recent years, new encryption programs like Tor, RedPhone, TextSecure, Cryptocat, and others have taken the spotlight - but the old guard of remailers and shared inboxes are still around. Alt. Anonymous.Messages is a stream of thousands of anonymous, encrypted messages, seemingly opaque to investigators. For the truly paranoid, there is no communication system that has better anonymity - providing features and resisting traffic analysis in ways that Tor does not. Or so is believed. After collecting as many back messages as possible and archiving new postings daily for four years, several types of analysis on the contents of alt.anonymous. messages will be presented and several ways to break sender and receiver anonymity explained. Messages will be directly and statistically correlated, communication graphs drawn, and we'll talk about what challenges the next generation of remailers and nymservs face, and how they should be designed.

FORENSIC FAILS - SHIFT + DELETE WON'T HELP YOU HERE

Eric Robi
Forensic Examiner, Elluma Discovery
Michael PErklin
Cyber Investigator

Forensic fails illustrates the rather comedic attempts at "anti-forensics" by inept computer users trying to hide their tracks. We will recount real-life stories about folks whose level of hacker-mojo might aspire to 1337 status but fall a little short. This talk covers why and how these fails happened and illustrate the forensic artifacts and the techniques used to analyze them.

THE DAWN OF WEB 3.0: WEBSITE MAPPING AND VULNERABILITY SCANNING IN 3D, JUST LIKE YOU SAW IN THE MOVIES

Teal Rogers
Owner, Trinary Software
Alejandra Caceres
Owner, Hyperion Gray, LLC.

Remember that scene in Hackers where Jonny Lee Miller and Angelina Jolie get a bunch of hackers to attack Fisher Steven's network through vulnerabilities that they find while flying (literally) through Fisher's network? Even though it had no basis in reality at the time, it was still pretty awesome. This presentation will be like that, except real.

This highly demo-focused presentation will unleash the next generation of web application visualization and security flaw detection. Created as part of DARPA's Cyber Fast Track, we have developed a completely awesome way of visualizing, in 3D, how massive numbers of web applications across the Internet are interconnected. This visualization engine provides a simple yet beautiful view of web applications and their vast, sprawling interconnections, all the while incorporating web application vulnerabilities into the visual metadata.

BUILDING AN ANDROID IDS ON NETWORK LEVEL

Jaime Sanchez
A3SEC

Being popular is not always a good thing and hereis why. As mobile devices grow in popularity, so do the incentives for attackers. Mobile malware and threats are clearly on the rise, as attackers experiment with new business models by targeting mobile phones. Nowadays, several behavior-based malware analysis and detection techniques for mobile threats have been proposed for mobile devices. We'll show how we built a new detection framework that will be the first open source Android IDS on network level.

This open source network-based intrusion detection system and network-based intrusion protection system has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks, featuring: Protocol analysis, Content searching and Content matching.

In IDS/IPS mode, the program will monitor network traffic and analyze it against a rule set defined by the user, and then perform a specific action based on what has been identified. With the help of custom build signatures, the framework can also be used to detect probes or attacks designed for mobile devices, fool and cheat operating system fingerprinting attempts (like nmap or p0f), server message block probes, etc.

SAFETY OF THE TOR NETWORK: A LOOK AT NETWORK DIVERSITY, RELAY OPERATORS, AND MALICIOUS RELAYS

Runa A. Sandvik
Developer, The Tor Project

Rumor has it that the Tor network is a CIA honeypot, that all relays are malicious, and that only bad people use Tor to do bad things online. How much of this is true? How much can we say about the safety of the network?

The safety of the Tor network has been a much discussed topic ever since the onion routing network was deployed in September 2002. This talk aims to answer the following questions: (1) How much diversity does the network really have?, (2) Who runs the relays in the Tor network?, and (3) What is being done about malicious relays?

THE DARK ARTS OF OSINT

Noah Schiffmann
Skydog

The proliferation and availability of public information has increased with the evolution of its dissemination. With the constant creation of digital document archives and the migration towards a paperless society, vast databases of information are continuously being generated. Collectively, these publicly available databases contain enough specific information to pose certain vulnerabilities. The actionable intelligence ascertained from these data sources is known as Open Source Intelligence (OSINT).

Numerous search techniques and applications exist to harvest data for OSINT purposes. Advanced operator use, social network searches, geospatial data aggregation, network traffic graphs, image specific searches, metadata extractors, and government databases, provide a wealth of useful data. Furthermore, applications such as FOCA, Maltego, and SearchDiggity, in addition to custom site API integration, yield powerful search queries with organized results.

PRESENTATIONS

Fluency in OSINT methodologies is essential for effective online reconnaissance, although a true mastery requires further mathematical investigation. The use of statistical correlation can often reveal hidden data relationships. Linkage attacks, inferential analysis, and deductive disclosure can exploit improperly sanitized data sets. These techniques can ultimately lead to data re-identification and de-anonymization, thus exposing personal information for exploitation. We will demonstrate our mathematical algorithm for data identification by attacking publically available anonymized datasets and revealing hidden personal information.

BRUCE SCHNEIER ANSWERS YOUR QUESTIONS

Bruce Schneier

Security topics preferred. Last year he gave away galley copies of his latest book to anyone who asked a question. We don't know what he's going to do this year.

HOW MY BOTNET PURCHASED MILLIONS OF DOLLARS IN CARS AND DEFEATED THE RUSSIAN HACKERS

Michael Schrenk

This is the true story of a botnet that created a competitive advantage for a car dealership. This dealership found a website that offered returned lease vehicles—great cars for their inventory—but bad web design and heavy competition from other automotive dealerships made the website useless. In response, a botnet was developed to make automotive purchases with machine precision. With the bot, they could acquire any cars they wanted, without interference from competing dealerships. During its one-year life, this botnet autonomously acquired many millions of dollars in cars. Along the way, it successfully adjusted to competition from a similar bot developed by Russian hackers while maintaining a sufficiently low profile to "stay below the radar" of everyone involved.

EXAMINING THE BITSQUATTING ATTACK SURFACE

Jaeson Schultz

Threat Research Engineer, Cisco Systems

Bit errors in computer memory, when they occur in a stored domain name, can cause Internet traffic to be directed to the wrong Internet location potentially compromising security. When a domain name one bit different from a target domain is registered, this is called "bitsquatting". This presentation builds on previous work in this area presented by Artem Dinaburg at Blackhat 2011. Cisco's research into bitsquatting has revealed several previously unknown vectors for bitsquatting. Cisco has also discovered several new mitigations which do not involve installation of error correcting memory, nor the mass registration of bitsquat domains. In fact some of the new mitigations have the potential to render the problem of bitsquatting to the dustbin of history.

HACKING WIRELESS NETWORKS OF THE FUTURE: SECURITY IN COGNITIVE RADIO NETWORKS

Hunter Scott

M2M, IoT, whatever buzzword you want to use, telecoms are predicting and preparing for a huge increase in embedded, connected devices within the next 10 years and predict spectrum utilization will increase even faster in the next 5 years. One of the ways this growth will be addressed is with cognitive radio networks. This talk will discuss the new kinds of security issues that are faced by these networks, particularly TV Whitespace. It will NOT presuppose knowledge of RF engineering and will work up from the basics of what cognitive radio is to the security challenges it faces, many of which are not yet solved. It will also release a new hardware platform for building and breaking cognitive radio networks.

MAKING OF THE DEF CON DOCUMENTARY

Jason Scott

Director, DEF CON: The Documentary

Rachel Lovinger

Producer, DEF CON: The DocumentarY

Early in 2012, to commemorate the 20th year of the conference, Jason Scott was asked if he would be interested in filming a documentary about DEF CON, whose policies and attendees have traditionally rejected media scrutiny and access. He was interested. Working with his producer, Rachel Lovinger, and a crew of six, Jason filmed for most of 2012, including five 20-hour days in Las Vegas last year, and then spent another 9 months editing 278 hours of footage into what has become DEF CON: The Documentary. The finished film will premiere at DEF CON XXI. Jason and Rachel will provide a look behind the scenes: discussing the planning and production process for this immense project, the ups and downs, and the learned lessons. Plus, we'll show some of the stranger footage you won't get to see in the final film.

ALL YOUR RFZ ARE BELONG TO ME - HACKING THE WIRELESS WORLD WITH SOFTWARE DEFINED RADIO

Balint Seeber

Spench.net

Ever wondered what traffic is flowing through the many satellites in orbit above you? Have you wanted to intercept RADAR signals from air traffic control and visualise your local airspace in real-time on a 3D map? While youire at it, check how many faults have been reported by the next plane youill be travelling on (e.g. do the toilets work?). How about tracking down the source of a clandestine radio transmission that is interfering with your favourite channel, or probing the signals on your cable modem connection? If you have ever wanted to reverse engineer such systems, this is for you!

I will show how to analyse and hack RF communications systems using open source software and cheap radio hardware. The focus will be on how to use Software Defined Radio to create: a digital satellite demodulator for blind signal analysis, a souped-up Mode S aviation transponder/ACARS receiver with an Internet-enabled smooth-streaming Google Earth front-end, and a Radio Direction Finder.

A PASSWORD IS NOT ENOUGH: WHY DISK ENCRYPTION IS BROKEN AND HOW WE MIGHT FIX IT

Daniel Selifonov

Since the publication of the cold boot attack on software disk encryption 5 years ago, there has been little progress on developing countermeasures and implementing defenses in the disk encryption technologies already in wide use. Furthermore, many users of full disk encryption have physical security habits that fall outside the security models of disk encryption software and thus are more vulnerable than they realize. After examining a set of effective, easily executable, attacks on off- the-shelf disk encryption, and contextualizing them in x86 system architecture, we examine recent research on means of mitigating these attacks. By integrating AES new instructions, x86 debugging registers, encrypted RAM, IOMMU, and the TPM into a combined encryption system, the difficulty of executing a successful attack is raised significantly. We will examine the construction of this system in detail, and, at a higher level, the role of full disk encryption in assuring meaningful security in the face of physical access. Source to an experimental version of the system will be made available.
.

EMET 4.0 PKI MITIGATION

Neil Sikka

Software Security Engineer, Microsoft

Microsoft EMET is a free Mitigation tool. In addition to its memory corruption exploit mitigations, a newly introduced feature is the PKI mitigation. This mitigation implements x509 certificate pinning to prevent usage of forged certificates in HTTPS sessions in the web browser. This talk is technical as it demos EMET in action and explains how the PKI mitigation works. .

DRAGONLADY: AN INVESTIGATION OF SMS FRAUD OPERATIONS IN RUSSIA

Ryan W. Smith

Senior Research And Response Engineer, Lookout Mobile Security

Tim Strazzere

Lead Research And Response Engineer, Lookout Mobile Security

One of the top types of Android malware are trojans that claim to provide a useful service, but instead send SMS messages to premium shortcodes, charging the victims and putting money directly into the attackers' hands. We've seen a steady increase in this type of malware over the past years, and recently we've seen an increase in sophistication of obfuscation and distribution techniques as well. By investigating certain families of malware over time, we've seen encryption, code level obfuscation, on-demand build systems, and weekly code release cycles become more common. It became clear that there was significant organization and investment of both time and money behind several of these malware families, so we began following leads to find out how far the rabbit hole goes.

This presentation will show key findings and methods of this investigation into top Android malware distributors operating in Russia and the surrounding region. The investigation includes the discovery of 10's of thousands of bot-controlled twitter accounts spreading links to this type of SMS fraud malware, tracing distribution through thousands of domains and custom websites, and the identification of multiple "affiliate web traffic monetization" websites based in Russia which provide custom Android SMS fraud malware packaging for their "affiliates". During this investigation we have mapped out an entire ecosystem of actors, each providing their own tool or trade to help this underground community thrive.

Come out to this talk to find out how just how much effort and manpower is invested in defrauding Android users through this type of SMS trojan malware, and the types of organizations that are behind it.

EVOLVING EXPLOITS THROUGH GENETIC ALGORITHMS

soen

Hacker For Team Vanned & Consultant for Securedna

This talk will discuss the next logical step from dumb fuzzing to breeding exploits via machine learning & evolution. Using genetic algorithms, this talk will take simple SQL exploits and breed them into precision tactical weapons. Stop looking at SQL error messages and carefully crafting injections, let genetic algorithms take over and create lethal exploits to PWN sites for you!

BACKDOORS, GOVERNMENT HACKING AND THE NEXT CRYPTO WARS

Christopher Soghoian

Principal Technologist, Privacy & Technology Project, ACLU

The FBI claims it is going dark. Encryption technologies have finally been deployed by software companies, and critically, enabled by default, such that emails are flowing over HTTPS, and disk encryption is now frequently used. Friendly telcos, who were once a one-stop-shop for surveillance can no longer meet the needs of our government. What can the FBI and other agencies do to preserve their spying capabilities?

Part of the answer is backdoors: The FBI is rallying political support in Washington, DC for legislation that will give it the ability to fine Internet companies unwilling to build surveillance backdoors into their products. Even though interception systems prove to be irresistible targets for nation states, the FBI and its allies want to make our networks less secure, not more.

The other solution embraced by the FBI is hacking, by the government, against its citizens. A team of FBI agents and contractors, based in Quantico, Virginia have developed (and acquired) the capabilities to hack into systems, deliver malware capable of surreptitiously enabling a computer's webcam, collecting real-time location data, as well as exfiltrating emails, web browsing records and other documents.

While politicians are clearly scared about hacks from China, our own law enforcement agencies are clearly in the hacking business. What does this mean for the current, heated debate about cybersecurity and our ability to communicate security?

HOW TO HACK YOUR MINI COOPER: REVERSE ENGINEERING CONTROLLER AREA NETWORK (CAN) MESSAGES ON PASSENGER AUTOMOBILES

Jason Staggs

Grad Student And Research Assistant, University of Tulsa

This presentation introduces the underlying protocols on automobile communication system networks of passenger vehicles and evaluates their security. Although reliable for communication, vehicle protocols lack inherit security measures. This work focuses strongly on controller area networks (CANs) and the lack of authentication and validation of CAN messages. Current data security methods for CAN networks rely on the use of proprietary CAN message IDs along with physical boundaries between the CAN bus and the outside world. As we all know, security through obscurity is not true security. These message IDs can be reverse engineered and spoofed to yield a variety of results. This talk discusses methods for reverse engineering proprietary CAN messages. These reverse engineered messages are then injected onto the CAN bus of a 2003 Mini Cooper with the help of cheap Arduino hardware hacking. Additionally, a proof of concept will be demonstrated on how to build your own rogue CAN node to take over a CAN network and potentially manipulate critical components of a vehicle. The proof of concept demonstrates taking full control of the instrument cluster using the reverse engineering methods presented.

AN OPEN LETTER - THE WHITE HAT'S DILEMMA: PROFESSIONAL ETHICS IN THE AGE OF SWARTZ, PRISM AND STUXNET

Alex Stamos

Co-Founder and CTO, iSEC Partners

The information security world is constantly buffeted by the struggle between whitehats, blackhats, antisec, greenhats, anarchists, statists and dozens of other self-identified interest groups. While much of this internecine conflict is easily dismissed as "InfoSec Drama", the noise of interpersonal grudges often obscures a legitimate and important debate: what is the definition of "security" to whom do we provide it?

The last several years have made this external argument and internal ethical debate much more difficult to individuals gainfully employed in InfoSec, thanks to politically motivated prosecutions, domestic surveillance by democratic societies, and even the direct targeting of large companies by their home nations. What rules should guide us in deciding what jobs to take, what services to provide, and our actions in the public sphere?

This talk does not have the answers, but hopefully can help the overall community ask the right questions. We will begin with the speaker's personal experience working for Aaron Swartz's defense and on several high-profile civil cases. We will then discuss recent events in offensive cyber-warfare and the new dilemmas this poses for defenders. Finally, the speaker will present one possible framework for ethical decision making in such a complicated time, and will unveil an effort to affect change in the White Hat community.

COLLABORATIVE PENETRATION TESTING WITH LAIR

Tom Steele

Senior Security Consultant, Fishnet Security

Dan Kottmann

Security Consultant, Fishnet Security

Lair is an open-source project developed for and by pentesters. Built on Meteor and Node.js with a dash of Python, Lair is a web application that normalizes, centralizes, and manages diverse test data from a number of common tools including Nmap, Nessus, Nexpose, and Burp. Unlike existing alternatives, Lair encourages team-based collaboration by automatically pushing updates to team members in real time. Paired with it's workflow and documentation management,

PRESENTATIONS

Lair offers a single solution for performing a detailed, thorough penetration test individually or as a team in a manner that has not been done before.

DNS MAY BE HAZARDOUS TO YOUR HEALTH

Robert ‘Tick’ Ficke
Security Researcher

The largest manufacturer of laptops, one of the largest consulting firms, and a big data behemoth all walk into a bar...

His research explores many self-inflicted gaps that continue to plague even the largest companies. These gaps are often seen as trivial and ignored, thus making all of their DNS investments lead to a false sense of security. Too much effort and trust go into vendor solutions when ‘common sense’ and ‘due diligence’ were never deliverables requested in the RFP. Before we invest in securing our domains, it may be wise to ensure we own them. Before we harden our resolvers to prevent poisoning, maybe we should ensure our clients are querying what is expected. Before we make operational decisions about how client resolver settings should be configured, maybe should consider the consequences to DNS behavior. Before we call DNS secure, maybe we should understand what it is doing.

PREDICTING SUSCEPTIBILITY TO SOCIAL BOTS ON TWITTER

Chris Sumner
Randall Wald

Are some Twitter users more naturally predisposed to interacting with social bots and can social bot creators exploit this knowledge to increase the odds of getting a response?

Social bots are growing more intelligent, moving beyond simple reposts of boilerplate ad content to attempt to engage with users and then exploit this trust to promote a product or agenda. While much research has focused on how to identify such bots in the process of spam detection, less research has looked at the other side of the question—detecting users likely to be fooled by bots.

This talk provides a summary of research and developments in the social bots arms race before sharing results of our experiment examining user susceptibility.

EDS: EXPLOITATION DETECTION SYSTEM

Amr Thabet
Malware Researcher, Q-CERT

In the last several years, exploits have become the strongest weapons in cyber warfare. Exploit developers and vulnerability researchers have now become the nuclear scientists of the digital world. OS Companies and third party companies have created several security mitigation tools to make it harder to use these vulnerabilities and have made exploit creation harder.

In this presentation, I will talk about a new security mitigation tool which is based on the co-operation of several mitigations to cover their weaknesses. It’s based on monitoring the memory changes without decreasing the performance of the running application and creates a multi-layer protection with regular mitigations.

THE GOVERNMENT AND UFOS: A HISTORICAL ANALYSIS BY RICHARD THIEME

Richard Thieme

This talk is about the ways the many components of governments interact and respond to challenging and anomalous events--highly relevant to hacking by all definitions and at all levels. If you donit know the lay of the land, you can not engage in appropriate research and reconnaissance, counter-measures, and operations.

The proliferation of reliable reports of unidentified flying objects from the 1940s forward represented just such a challenge. The phenomenon was anomalous, well-documented, and certainly challenging because, as Major General John Samford said, “credible people have seen incredible things.”

The UFO History Group includes some of the best researchers in the field. Richard Thieme was privileged to be invited to join the group and their project which resulted, after nearly 5 years of work, in “UFOs and Government: A Historical Inquiry,” an outstanding work of historical scholarship that nevertheless reads like a fascinating detective story. In almost 600 pages and with nearly 1000 citations, the work illuminates the response of the government since the early 1940s. how and why policies were set, and how they were executed. The book has been recommended by CHOICE, the primary resource for academic libraries, for inclusion by libraries at all levels because the book stands out as “an exception” in a field filled with speculation (there is virtually none in this book). Other reviews say, “this is the best book about the UFO phenomena that was ever written” and “UFOs and Government is a triumph of sober, conscientious scholarship unlikely to be equaled for years to come.”

You have never heard a talk like this – about a subject that has been ridiculed and marginalized intentionally for sixty years as a matter of policy and politics. As Don Quixote said, “insanity is seeing things as they really are.” This speech uses UFO phenomena as dye in the arteries of “how things really are.”

BOUTIQUEKIT: PLAYING WARGAMES WITH EXPENSIVE ROOTKITS AND MALWARE

Josh ‘MONK’ Thomas
Applied Research Scientist, Accuvant

“Theoretical” targeted rootkits need to play by different rules than the common malware that ends up filling our inboxes with spam and attempting to steal our CC numbers... The costs involved of getting popped are huge in comparison, the value is in the secrecy of being truly hidden and embedded for the long term.

I’ve spent the past year considering what the next level of rootkits would look like and how we can protect ourselves against them. This talk will cover a handful of advanced hiding mechanisms at a technical level. The talk will also touch on legal implications and existing frameworks for expensive advanced threats.

C.R.E.A.M. CACHE RULES EVIDENTLY AMBIGUOUS, MISUNDERSTOOD

Jacob Thompson

Common wisdom dictates that web applications serving sensitive data must use an encrypted connection (i.e., HTTPS) to protect data in transit. Once served, that same sensitive data must be protected at rest, either through encryption, or more appropriately by not storing the sensitive data on disk at all. In the past, web browser disk caching policies maintained a distinction between HTTP and HTTPS requests, typically refusing to cache HTTPS requests. With today’s bandwidth- and performance-hungry AJAX and HTML5 applications, most modern browsers treat all content (including HTTPS) as safe to cache to disk unless explicitly restricted by the server. This silent “shift” of responsibility from browser to web-application server has eluded both secure web-application and safe-browsing paradigms, leaving consumers exposed. Even OWASP recommended guidelines for creating secure web applications are wrong regarding this topic [1].

We tested over thirty sites that provide personal financial, health, and insurance-related information to determine what, if any, sensitive information was cached to disk and the results were surprising. Over 70% of tested sites cached sensitive information, ranging from account balances to bank-check images, bank statements, and full credit reports.

We will discuss not only the technical details of these caching vulnerabilities, but also the history behind the “shift” in cache policy responsibility, the breakdown in conventional wisdom concerning web application and web-browser security policies, the ramifications of caching PII to disk, and the potential widespread violation of most compliance standards, including PCI, HIPAA, SOX, and government standards such as FIPS or Common Criteria.

INSECURITY - A FAILURE OF IMAGINATION

Marc Weber Tobias
Investigative Attorney And Security Specialist, Security.org
Tobias Bluzmanis
Security Specialist, Security.org

Homeowners, apartment complexes, and businesses throughout the United States and Canada have purchased locks from one of the leading manufacturers in the country in the belief that they were secure. Advertising represents they are the highest grade of residential security available as a result of security ratings from different Standards organizations. While the design of this lock effectively resists certain forms of covert and forced entry that are common with other mechanical cylinders, there are also what we perceive as serious design flaws that will allow these locks to be opened, bypassed, or decoded in seconds. Because this is one of the most popular locks in America, the consumer needs to understand the inherent security vulnerabilities in order to assess their risk.

In this presentation we analyze the design of this lock and earlier similar designs implemented by other manufacturers. The focus is on a failure of the design engineers to understand different methods of bypass and to protect against them, and why standards and what they purport to define may be misleading and misrepresent the real security of a product.

HTTP TIME BANDIT

Vaagn Toukharian
Principal Engineer, Qualys
Tigran Gevorgyan
Engineering Manager, Qualys

While web applications have become richer to provide a higher level user experience, they run increasingly large amounts of code on both the server and client sides. A few of the pages on the web server may be performance bottlenecks. Identifying those pages gives both application owners as well as potential attackers the chance to be more efficient in performance or attack. We will discuss a tool created to identify weaknesses in the web application by submitting a series of regular requests to it. With some refinement and data normalizations performed on the gathered data, and then performing more testing based on the latter, it is possible to pinpoint the single most (CPU or DB) resource-consuming page of the application. Armed with this information, it is possible to perform more efficient DOS/DDOS attacks with very simple tools. The presentation will be accompanied by demos of the tool performing testing and attacking on various targets. The tool will be published for the interested researchers to play with.

THE GROWING IRRELEVANCE OF US GOVERNMENT CYBERSECURITY INTELLIGENCE INFORMATION

Mark Weatherford
Principal, The Chertoff Group

The rapidly changing threat landscape has finally provided relevant business justification for commercial companies to invest in developing cybersecurity intelligence that used to be the domain of the government – and they are doing it at a pace that is making the value of government “Classified” cybersecurity information increasingly irrelevant. The organic intelligence being developed by private companies and the informal cybersecurity intelligence coming out of the research community and some “Invitation Only” or “You’re Not Invited” groups is simply more actionable and more valuable than that provided by the government. While the federal government will always, and should always, have important visibility of the threat, the evolution of technology is giving the private sector the means to develop sophisticated, high quality information that rivals the government.

PROWLING PEER-TO-PEER BOTNETS AFTER DARK

Tillmann Werner
Crowdstrike, Inc.

Peer-to-peer botnets have become the backbone of the cybercrime ecosystem. Due to their distributed nature, they are more difficult to understand and contain than traditional botnets. To combat this problem, we have developed the open-source framework *prowler* for peer-to-peer botnet tracking and node enumeration. It combines efficient crawling strategies with the ability to plug in implementations for custom application layer protocols. In this talk, attendees will learn how to use prowler to reconnoiter and track peer-to-peer botnets. We will show some real-world examples, interpret the results, and discuss pitfalls and challenges. We will then examine how these results can be used in attempts to attack and take over peer-to-peer botnets.

REALITY HACKERS

Rebecca Wexler
Director/Producer Yale Visual Law Project
Paul Sanderson
Director/Producer Our Town Films

Reality Hackers. Technology, wit, and hacker culture fuse in an electrified movement for digital freedom. Meet the activists who make and break technology to ensure free speech and private communication for political dissidents, and to combat global censorship. This film gives a behind-the-scenes look at those who are sometimes characterized as outlaws, but who may be the vanguard defenders of freedom for all. Partially shot at DEF CON 19, the film shows the real people behind the headlines as they navigate the complexities of modern geo-political struggles. Featuring over eight DEF CON speakers, multiple CCC participants, and members of the German Pirate Party, Reality Hackers is an intimate portrait of characters who use technology to alter the world.

DEFEATING INTERNET CENSORSHIP WITH DUST, THE POLYMORPHIC PROTOCOL ENGINE

Brandon Wiley
Researcher, Step Three: Profit!

The greatest danger to free speech on the Internet today is filtering of traffic using protocol fingerprinting. Protocols such as SSL, Tor, BitTorrent, and VPNs are being summarily blocked, regardless of their legal and ethical uses. Fortunately, it is possible to bypass this filtering by reencoding traffic into a form which cannot be correctly fingerprinted by the filtering hardware. I will be presenting a tool called Dust which provides an engine for reencoding traffic into a variety of forms. By developing a good model of how filtering hardware differentiates traffic into different protocols, a profile can be created which allows Dust to reencode arbitrary traffic to bypass the filters.

Dust is different than other approaches because it is not simply another obfuscated protocol. It is an engine which can encode traffic according to the given specifications. As the filters change their algorithms for protocol detection, rather than developing a new protocol, Dust can just be reconfigured to use different parameters. In fact, Dust can be automatically reconfigured using examples of what traffic is blocked and what traffic gets through. Using machine learning a new profile is created which will reencode traffic so that it resembles that which gets through and not that which is blocked. Dust has been created with the goal of defeating real filtering hardware currently deployed for the purpose of censoring free speech on the Internet. In this talk I will discuss how the real filtering hardware work and how to effectively defeat it.

BYOD PEAP SHOW

Josh Yavor
FSEC Partners

The onslaught of Bring Your Own Device(s) in recent years places a new focus on the security of wireless networks. In “The BYOD PEAP Show”, Josh Yavor explores fundamental flaws in one of the most common and widely supported 802.1x authentication protocols used by countless corporate WPA2-Enterprise networks today. A series of events in the recent past created a situation in which PEAP can no longer be used safely. In this talk, we will re-trace this path and investigate how the combination of BYOD, new technology and new tools led to this situation. A live demonstration with audience participation will punctuate the danger of supporting PEAP. Attendees will leave with an understanding of the underlying flaws, methods of exploitation, a set of tools and most importantly, how to secure WPA2-Enterprise

PRESENTATIONS

networks that currently support PEAP. A new tool, peapshow, will be released after DEF CON and will make testing and exploitation of this issue truly trivial.

ANDROID WEBLOGIN: GOOGLE'S SKELETON KEY

Craig Young
Vert Security Researcher, Tripwire

Millions of businesses worldwide trust in Google Apps to run their organization's domain. The life-blood of these organizations is routinely stored with Google accounts and accessed with mobile devices. This talk explores how an adversary can parlay the compromise of a single Android device into a complete Google apps domain takeover. The attack vectors explored in this talk make use of various design considerations made by Google to enhance the user-experience and can be equally utilized with malware or physical device access.

Several iterations of malicious Android applications were created using these techniques. The apps were then analyzed with multiple Android Anti-Virus products and subsequently published in Google's Play Store. The PoC iterations and analysis results provide some insight into the state of Google's Bouncer and Android malware analysis at the end-point.

The final part of the talk is aimed at identifying best practices to minimize risk as well as guidelines for recovering from security incident.

HACKING DRIVERLESS VEHICLES

Zoz
Cannytrophie Design

Are driverless vehicles ripe for the hacking? Autonomous and unmanned systems are already patrolling our skies and oceans and being tested on our streets and highways. All trends indicate these systems are at an inflection point that will show them rapidly becoming commonplace. It is therefore a salient time for a discussion of the capabilities and potential vulnerabilities of these systems.

This session will be an informative and light-hearted look at the current state of civil driverless vehicles and what hackers or miscreants might do to mess with them. Topics covered will include common sensors, decision profiles and their potential failure modes that could be exploited. With this talk Zoz aims to both inspire unmanned vehicle fans to think about robustness to adversarial and malicious scenarios, and to give the paranoid false hope of resisting the robot revolution. He will also present details of how students can get involved in the ultimate sports events for robot hacking, the autonomous vehicle competitions.

MOVIE NIGHT
with the Dark Tangent

Watching movies with DT on Saturday night is a time-honored DEF CON tradition. Let the rubes brave the heat of the Strip, join us in air-conditioned comfort to watch a movie and meet some of the filmmakers. The movies are shown in Track 2!

The Liar Game: The Final Stage

In the theme of not knowing who to trust or who to believe I think the social engineers will really enjoy this one. With the shifting alliances and multiple rounds of who can betray who the best for monetary rewards contestants participate in the high stakes "Liar Game" to see who is best of the best. Like survivor but for human hackers. I would love to show you what came before this movie, but unfortunately that was several seasons of TV episodes. This is the first of two movies in the series, and also the best of the two. Enjoy!

SATURDAY NIGHT AT 21:00 IN TRACK 2

Reality Hackers

Reality Hackers. Technology, wit, and hacker culture fuse in an electrified movement for digital freedom. Meet the activists who make and break technology to ensure free speech and private communication for political dissidents, and to combat global censorship. This film gives a behind-the-scenes look at those who are sometimes characterized as outlaws, but who may be the vanguard defenders of freedom for all. Partially shot at DEF CON 19, the film shows the real people behind the headlines as they navigate the complexities of modern geo-political struggles. Featuring over eight DEF CON speakers, multiple CCC participants, and members of the German Pirate Party, Reality Hackers is an intimate portrait of characters who use technology to alter the world.

SATURDAY NIGHT AT 20:00 IN TRACK 2

DEF CON VENDORS

ACLU

The ACLU is our nation's guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country.

The ACLU's wide-ranging work in digital privacy focuses on expanding the right to privacy, increasing the control that individuals have over their personal information, and ensuring that civil liberties are enhanced rather than compromised by new advances in science and technology. Our work in this field includes freedom of expression online, privacy of electronic information, journalists' rights, scientific freedom, and openness in the courts. Make sure to visit our booth in the vendor area to learn more, and join us on Friday night to Party Like It's 1986!

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

This is our 5th year as a vendor at DEF CON! We have added over 150 new tools in our catalog. 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 5th year at DEFCON by showcasing our own line of lock picks!! This year, we will feature our Black Diamond sets and our Ruby sets. Our sister company, Ace Hackware, will also be joining us at the booth. So come see us for all your Lock Pick Sets, Bump Keys, Clear Practice Locks, Jackknife Pick Sets, Hackware, and more. As always, a percentage of our proceeds will go to the Miracle Match Foundation. Long live Barcode!

ELECTRONIC FRONTIER FOUNDATION

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We defend free speech on the Internet, fight illegal surveillance, support freedom-enhancing technologies, promote the rights of digital innovators, and work to ensure that the rights and freedoms we enjoy are enhanced, rather than eroded, as our use of technology grows.

ELECTRIC SHEEP PRESS

We are the Electric Sheep Scribes, and we bring you Electric Sheep Press: a world-changing publishing company. We'll make you laugh. We'll make you cry. We'll pull the wool back from over your eyes.

Traditional fiction publishing has been on life-support for far too long. Electric Sheep Press (ESP to the cool kids) is ready to pull the plug. Founded by the Electric Sheep Scribes -- Cloudy, Tasky, and Spelly -- ESP is dedicated to two things: providing technology-savvy audiences with high-quality science fiction and fact ("hacker entertainment," if you will), and paying writers percentages that would make traditional publishers choke.

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)

THE HACKER ACADEMY

The Hacker Academy (THA) is an online learning platform for ethical hacking and penetration testing that provides real world tools, concepts, and 24/7 hands on training in a cloud based environment. The Hacker Academy provides a true understanding of how hacking actually works and what it feels like from a "bad guys" perspective, which arms you with the knowledge to protect your own systems. THA is a division of MAD Security, a boutique information security training firm that focuses on improving the security of their clients through improvement in user behavior and the skills of their technical staff. Improve your humans, Improve your security.

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

HackerStickers.com offers the best in hacker threads (clothing up to 5XL!), caffeine, technology and mind bending tools for all trades including lock picking! Official Vendor for DEF CON swag after the con! So click us out, join our mailing list, follow us on facebook and twitter for the latest releases, specials and deals!

HACKER WAREHOUSE

HackerWarehouse.com strives to be your one-stop shop for all your computer security needs from defense to offense. 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.

A portion of each sale will go back to support the information security community. From tool developers to non-profits, we only partner with people or organizations that enhance and contribute the community.

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.

KEYPORT

Keyport has reinvented the conventional keychain by consolidating your most important personal items (keys, USB flash drive, mini-light, bottle opener, barcode holder, and more in development) into a single, streamlined device that replaces your keychain. This is our first year at DEFCON and we will be selling our brand new Keyport Slide 2.0 and full line of Keyport Blades, Inserts, and Accessories at 10% off. Bring your keys and get ported on the spot.

KINETEKA SYSTEMS

Kineteka Systems designs and manufactures specialty high-tech products as well as resells a variety of niche electronics for the growing Maker/Hacker movement.

LBGFX

Customize T shirts & Stickers on the spot at DEF CON 21

Purveyors of fine hacker-related merchandise

NO STARCH PRESS

No Starch Press publishes books for geeks of all ages. We focus on computer security, programming, open source, LEGO, and science. Our titles have personality, our authors are passionate, and we read and edit every book that bears our name.

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!

PWNIE EXPRESS

Pwnie Express specializies in bleeding edge hardware and software for penetration testers including the Pwn Plug, the Power Pwn and the Pwn Pad. Pwnie Express devices use covert tunnels and cellular connections to maintain an encrypted, firewall-busting backdoors into target networks. Stop by the booth for Pwnie swag and learn about the new tricks they're up to.

SECURENINJA

SecureNinja provides expert Cybersecurity Training and Certification & Security Services. Training Courses included Cyber Intelligence, Cyber Counterintelligence & Cybercrime, Advanced Offensive Hacking and Penetration Testing, Advanced Offensive Mobile Application Hacking, CISSP, CEH v8, Computer Forensics, CISM, Cloud Security, Cyber Tools and Analysis Hands-on Workshop and more. Our classes come in flexible formats (Boot Camp, Live Online, Evenings, Weekends, On-site and Self-Paced Computer Based Training) to meet your busy schedule or organizational need. Secure Ninja services/consulting specialize in governance, risk and compliance programs for government agencies including information assurance, IV&V security assessments, and Cybersecurity solutions. SecureNinja is celebrating our 10th anniversary; Stop by the SecureNinja booth at DEFCON and check out our latest Ninja Gear, view our newest product release, enter cool contests and to receive 30% off any SecureNinja training item.

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

SEREPICK THE LEADER IN SPECIALIZED EQUIPMENT & COVERT ENTRY TOOLS New tools and classics will be on display and available for sale. With a large selection of Custom Titanium toolsets, Entry Tools, Practice locks, Bypass tools and Urban Escape & Evasion hardware we guarantee we will have something you have not seen before, including items that until recently were only available for restricted purchase. The Full product range of SPARROWS lock picks and tools will also be available including their custom Un-Cuff Links and specialized bypass tools. All products will be demonstrated at various times and can be personally sampled for use and efficacy.

SHADOWVEX INDUSTRIES

Hacker culture relevant and artistic driven-limited production high quality girls & boys t-shirts and hoodies. Fresh DJ mixes of the finest electronic music from the underground. Zero-day custom vinyl stickers, posters and buttons and more of your favorite nick-hacks!

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.

STRATEGIC CYBER

Strategic Cyber is a purveyor of fine malware for your penetration testing and red teaming pleasure. Its flagship product, Cobalt Strike, runs social engineering campaigns, serves web drive-by attacks, and features a beaconing payload that escapes tricky egress situations. Brought to you by the creator of Armitage. http://www.advancedpentest.com/

TOOOL

The Open Organisation of Lockpickers will have available 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! All sales directly benefit TOOOL, a non-profit organization.

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)

UNKNOWN PREPPER

OMGWTFBBQ! When the SHTF, be smart and be prepared. Get in "The Know" at UNKNOWN.COM. Our mission is to help individuals and organizations plan, prepare and put into practice the insight, goods and skills needed to better survive The Unknown. UNKNOWN.COM works to provide a professional, true understanding of preparedness that is based upon the harsh reality of the day. We are also big fans of Zombie Films and Hacker culture, so come by and chat with us to get in The Know. And yes, we have cool swag as well.

CFP Review Board

Suggy

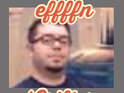
Chris is a security data guy at Hewlett-Packard, where he's been employed for over 18 years; albeit some of those years were with DEC and Compaq. For the past 14 years he has performed a variety of security roles, including worldwide Security Manager for HP's Imaging and Printing division. He has previously spoken on this area of research at conferences including DEF CON, BlackHat, 44CON, the European Conference on Personality and the International Conference on Machine Learning and Applications.

CJunky

has been a hacker since the late 80's and a DEF CON Goon for 15 years. He has more than 20 years experience working in infosec, much of which he either cant talk about, wont talk about, or simply cant remember because he was drunk. When not appearing at security conferences around the world, CJ can be found breaking things for @Lookout in SF.

Dead Addict

has been staff at DEF CON since its inception 21 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.



efffn

Maestro, DEF CON's Network Operation Center. 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.

Grifter

has been a DEF CON Goon for a lucky 13 years. He is currently the Senior Goon in charge of DEF CON Evening Event space. In previous lives he served as a Security, Vendor, and Skybox Goon, Coordinator of the DEF CON Movie Channel, and former Organizer of the Scavenger Hunt. He birthed the idea of the DEF CON Villages and DC Groups into the world, and he's not sorry about it. He has three black badges, for placing first in LosT's DEF CON Mystery Challenge, three years in a row.

Nikita

senior goon in charge of the DEF CON's call for papers, Speaker liaison, and overall conference administrator. Between reading and responding to several hundred papers she is often seen trolling the free world and raising a two year old son. A DEF CON attendee for the past ten years and a goon for eight, she's fully in love with this community despite the fact that many of you drive me insane. Most notably known for never sleeping from May to the end of July, an extensive hello kitty hoard, and a celebrated collection of animated gifs to express pleasure and disdain. You can subject yourself to her boring life narration via twitter @niki7a.

Lockheed

For 17 years, Lock organized, architected, and ran the DEF CON Network Operations Group. He continues the tradition that one never fully retires from DEF CON. Professionally he's worked in IT his entire career, doing everything from engineering, product development, web hosting, security, network design - you name it. In more recent times Lock has moved to the Dark Side (management). Currently Lock is head of Global IT for Sony PlayStation Worldwide Studios.

Roamer

Roamer is the (cross your fingers) soon to be retired Sr. Goon in charge of the DEF CON Vendor Area. His judgement must be called in to question since he has volunteered to Goon since DC 8, a sentence longer than many murderers serve. He has spoken at multiple DEF CONs (among other... lesser...conferences) starting at DC10. He has 15 years of InfoSec experience, mostly as a penetration tester doing red and blue team pen tests for three letter agencies, four letter agencies and other government agencies that have made him scream four letter words.

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). Attvending 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.

RussR

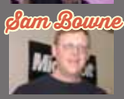
For 16 years, Russr has been involved in a number of different areas at the conference, including the vendor area, the contest area, Hardware Hacking Village, and more recently, the DEF CON Documentary. He works for his own company at Peak Security, doing research and fun, smaller projects. Russ also 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.

TW

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

Maxi 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 discovered vulnerabilities in different Web applications and several Microsoft products. He 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. A really 27/4 ToolsWatcher!



Sam Bowne

has been teaching computer networking and security classes at CCSF since 2000. He has given talks at DEFCON, BayThreat, LayerOne, Toorcon, and lightning talks at HOPE on Ethical Hacking, and taught classes and seminars at many other schools and teaching conferences. He has a PhD & lot of industry certs but still no CISSP.

HACKER JEOPARDY

RATED PG

FOR KIDS

Be Early! Bring your teams of 3, ready to go!

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

Saturday 2 - 3 pm
Crown Theatre
Game 1: 7 - 12 yrs old
Game 2: 13-17 yrs old

Compete for Prizes!

DON'T MISS THE FUN WITH YOUR HOST WINN, MISS KITTY AND MISS TIFFANY!

THURSDAY EVENTS

DEF CON 101

DC101 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 a n00b or a long time attendee, DC101 can start you on the path toward maximizing your DEF CON Experiences.

DEF CON 101

	Track 2	Track 3
10:00	**DC 101** *Panel*	**Hacker Law School** *Jim Rennie & Marcia Hofmann*
12:00	**Hacking Management** *Lockheed, Roamer & Naifx*	**Pentester's Toolkit** *Anch*
13:00	**The Ninjaneers** *Beaker & Flipper*	**Oil & Gas Infosec 101** *Aaron Bayles (AlxRogan)*
14:00	**Decrypting DEF CON** *LosT*	**Meet Pentoo** *ZeroChaos*
15:00	**Intro to Web Application Hacking** *Terrence "Tuna" Gareau*	**Wireless Penetration Testing 101 & Wireless Contesting** *DaKahuna & Rick Mellendick*

Hacker Karaoke

Thursday: 21:00-02:00, Friday: 21:00-02:00

Do you like music? Do you like performances? Want to BE the performer? Well trot your happy ass down to Hacker Karaoke, DEF CON's first 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 Bascule and OverDose as we put the casbah in "Rock the Casbah".

Toxic BBQ

Thursday, 16:00-22:00, Sunset park Area J

Every year thousands of Hackers and Computer Security Enthusiasts attend DEF CON the worlds largest underground hacking convention. Before the convention starts the Toxic BBQ is held. Its an event put together by attendees, not funded, organized, or sanctioned by the convention. Attendees donate thier time, money and food, and put together a huge kickoff to the con.

Every year attendance grows, and so does the selection of food, from Yak & Elk, to Ribs & Beer, the Toxic BBQ has something to offer everyone. Its not just a place to eat and drink, its a place to meet and greet your fellow attendees before the con.

Best of all, its free. You are encouraged to contribute something, whether it be food, donation, your cooking skills, or even a ride

the Summit

Returning for its 9th year, Vegas 2.0's theSummit is back to continue the revolution!

Held Thursday night between Black Hat and DEF CON, theSummit is an all ages fundraiser for the Electronic Frontier Foundation (EFF). As the week of conferences intensifies it is increasingly difficult to catch up to everyone you want to meet. theSummit is your chance to network with the industries 1337, have a drink with this year's speakers to ask some questions before their talk, or plot the weekend's shenanigans with new and old friends.

theSummit is a brilliant opportunity with live auction, full bar, door prizes, and entertainment by Dual Core & Dale Chase, DJ Jackalope and Ali Spagnola will be hosting her infamous Power Hour! As always, 100% of our proceeds are donated to the EFF.

$40 at the Door

**Each entry comes with a 1 year membership to the EFF and one raffle ticket.

**Additional donations to the EFF are always accepted.

Start Time: Thursday, August 1st, 2013 at 8:00pm Vegas 2.0: site.vegassummit.org/

End Time: Friday, July 27, 2010 at 2:00am Twitter: /effsummit

Location:Miranda Suite "Chill out lounge" Facebook: on.fb.me/Vegas20

EVENT SCHEDULE

20:00 - Doors Open

20:30 - Meet the Speakers

21:00 - Dual Core & Dale Chase

21:30 - Auction

22:30 - Ali Spagnola's Power Hour

23:30 - Raffle

00:00 - DJ Jakalope

01:00 - DJ Salor Gloom

Special thanks to Packet Barron, Ripshy, Dallas, Banasidhe, 0hm, Generic SuperHero, Beau, Krispy, Charlie, Gru, Str3tch, Vyrus, Savant 42, Kos, Blak Dayz, Night Owl, Fraggle, Matt, Salem, the Infamous Kevin, Valkyerie, Astcell, DJ Jackalope, Dual Core, Dale Chase, and of course the people behind the EFF that make us puke rainbows.

Friday August 2nd

	Penn & Teller	Track 1	Track 2	Track 3	Track 4
10:00	**Proliferation** *Ambassador Joseph R. DeTrani*	**Welcome & Badge Talk** *The Dark Tangent, LosT*	**I Can Hear You Now:** *Doug Deperry & Tom Ritter*	**Adventures in Automotive Networks and Control Units** *Charlie Miller & Chris Valasek*	**All Your RFz Are Belong to Me - Hacking the Wireless World with Software Defined Radio** *Balint Seeber*
11:00	**Torturing Open Government Systems for Fun, Profit and Time Travel** *Tom Keenan*	**The Growing Irrelevance of US Government Cybersecurity Intelligence Information** *Mark Weatherford*	**The Secret Life of SIM Cards** *Karl Koscher & Eric Butler*	**Hacking Driverless Vehicles** *Zoz*	
12:00	**Backdoors, Government Hacking and The Next Crypto Wars** *Christopher Soghoian*	**The Dirty South – Getting Justified with Technology** *David Kennedy & Nick Hitchcock*	**DragonLady: An Investigation of SMS Fraud Operations in Russia** *Ryan W. Smith & Tim Strazzere*	**10,000 Yen into the Sea** *Flipper*	**Making Of The DEF CON Documentary** *Jason Scott & Rachel Lovinger*
13:00	**ACL Steganography - Permissions to Hide Your Porn** *Michael Perklin*	**Prowling Peer-to-Peer Botnets After Dark** *Tillmann Werner*	**Offensive Forensics: CSI for the Bad Guy** *Benjamin Caudill* **Pwn'ing You(r) Cyber Offenders** *Piotr Duszynski*	**Business Logic Flaws In Mobile Operators Services** *Bogdan Alecu*	
14:00	**Protecting Data with Short-Lived Encryption Keys and Hardware Root of Trust** *Dan Griffin*	**Evil DoS Attacks and Strong Defenses** *Sam Bowne & Matthew Prince*	**MITM All The IPv6 Things** *Scott Behrens & Brent Bandelgar* **HTTP Time Bandit** *Vaagn Toukharian & Tigran Gevorgyan*	**Meet the VCs** *Panel*	**Ask the EFF: The Year in Digital Civil Liberties** *Panel*
15:00	**Google TV or: How I Learned to Stop Worrying and Exploit Secure Boot** *Amir Etemadieh & Panel*	**Kill 'em All – DDoS Protection Total Annihilation!** *Tony Miu & Wai-Leng Lee*	**How to use CSP to Stop XSS** *Kenneth Lee* **So You Think Your Domain Controller is Secure?** *Justin Hendricks*	**The ACLU Presents: NSA Surveillance and More** *Panel*	
16:00	**A Password is Not Enough: Why Disk Encryption is Broken and How We Might Fix It** *Daniel Selifonov*	**VoIP Wars: Return of the SIP** *Fatih Ozavci*	**Getting The Goods With smbexec** Eric MWm **Abusing NoSQL Databases** *Ming Chow*	**The Government and UFOs: A Historical Analysis** *Richard Thieme*	**Decapping Chips the ~~Easy~~ Hard Way** *Adam "Major Malfunction" Laurie & Zac Franken*
17:00		**Hacking Institutions : An American Folk Story** *Mudge*	**Examining the Bitsquatting Attack Surface** *Jaeson Schultz* **Please Insert Inject More Coins** *Nicolas Oberli*	**How my Botnet Purchased Millions of Dollars in Cars and Defeated the Russian Hackers** *Michael Schrenk*	

Saturday August 3rd

	Penn & Teller	Track 1	Track 2	Track 3	Track 4
10:00	**From Nukes to Cyber – Alternative Approaches for Proactive Defense and Mission Assurance** *Lt. Gen. Robert Elder USAF (Retired)*	**Dude, WTF in my car?** *Alberto Garcia Illera & Javier Vasquez Vidal*	**Do-It-Yourself Cellular IDS** *Sherri Davidoff & Panel*	**Predicting Susceptibility to Social Bots on Twitter** *Chris Sumner & Randall Wald*	**Insecurity - A Failure of Imagination** *Marc Weber Tobias & Tobias Bluzmanis*
11:00	**The Politics of Privacy and Technology: Fighting an Uphill Battle** *Eric Fulton & Daniel Zolnikov*	**The Road Less Surreptitiously Traveled** *Pukingmonkey*		**Fear the Evil FOCA: IPv6 attacks in Internet Connections** *Chema Alonso*	**Key Decoding and Duplication Attacks for the Schlage Primus High-Security Lock** *David Lawrence & Panel*
12:00	**Defeating Internet Censorship with Dust, the Polymorphic Protocol Engine** *Brandon Wiley*	**Home Invasion 2.0 : Attacking Network-Controlled Consumer Devices** *Daniel "UnicornFurnace" Crowley, Jennifer "SavageJen" Savage, & David "Videoman" Bryan*	**BoutiqueKit: Playing WarGames with Expensive Rootkits and Malware** *Josh 'Monk" Thomas*	**Legal Aspects of Full Spectrum Computer Network (Active) Defense** *Robert Clark*	**DEF CON Comedy Jam Part VI, Return of the Fail** *Panel*
13:00	**Privacy In DSRC Connected Vehicles** *Christie Dudley*	**RFID Hacking: Live Free or RFID Hard** *Francis Brown*	**Android WebLogin: Google's Skeleton Key** *Craig Young*	**We are Legion: Pentesting with an Army of Low-power Low-cost Devices** *Dr. Philip Polstra*	
			Building an Android IDS on Network Level *Jaime Sanchez*		
14:00	**Phantom Network Surveillance UAV / Drone** *Ricky Hill*	**Stalking a City for Fun and Frivolity** *Brendan O'Connor*	**Defeating SEAndroid** *Pau Oliva Fora*	**Pwn The Pwn Plug: Analyzing and Counter-Attacking Attacker-Implanted Devices** *Wesley McGrew*	**Hardware Hacking with Microcontrollers** *Panel*
			Doing Bad Things to 'Good' Security Appliances *Phorkus & Evilrob*		
15:00	**Safety of the Tor Network: a Look at Network Diversity, Relay Operators, and Malicious Relays** *Runa A. Sandvik*	**Hacking Wireless Networks of the Future: Security in Cognitive Radio Networks** *Hunter Scott*	**How to Hack Your Mini Cooper** *Jason Staggs*	**DC AWARDS**	**An Open Letter - The White Hat's Dilemma: Professional Ethics in the Age of Swartz, PRISM and Stuxnet** *Alex Stamos*
16:00	**De-Anonymizing Alt.Anonymous. Messages** *Tom Ritter*	**TBA**	**Electromechanical PIN Cracking with Robotic Reconfigurable Button Basher (and C3BO)** *Justin Engler & Paul Vines*	**PowerPreter: Post Exploitation Like a Boss** *Nikhil Mittal*	**Suicide Risk Assessment and Intervention Tactics** *Amber Baldet*
			Data Evaporation from SSDs *Sam Bowne*		
17:00		**Noise Floor: Exploring the World of Unintentional Radio Emissions** *Melissa Elliott*	**GoPro or GTFO: A Tale of Reversing an Embedded System** *Todd Manning & Zach Lanier*	**DNS May Be Hazardous to Your Health** *Robert Stucke*	**OTP, It Won't Save You From Free Rides!** *bughardy & Eagle1753*
			JTAGulator: Assisted Discovery Of On-Chip Debug Interfaces *Joe Grand aka Kingpin*		**How to Disclose or Sell an Exploit Without Getting in Trouble (Starts at 18:00)** *James Denaro*

Sunday August 4th

	Track 1	Track 2	Track 3	Track 4
10:00	**The Cavalry Isn't Coming: Starting the Revolution to Fsck it All!** *Nicholas J. Percoco & Joshua Corman*	**Made Open: Hacking Capitalism** *Todd Bonnewell*	**Exploiting Music Streaming with JavaScript** *Franz Payer*	**Defense by numbers: Making Problems for Script Kiddies and Scanner Monkeys** *Chris John Riley*
11:00	**The Dark Arts of OSINT** *Noah Schiffman & Skydog*	**gitDigger: Creating Useful Wordlists from Public GitHub Repositories** *Jamie Filson (Wix) & Rob Fuller (Mubix)*	**Java Every-Days: Exploiting Software Running on 3 Billion Devices** *Brian Gorenc & Jasiel Spelman*	**Resting on Your Laurels Will Get You Pwned: Effectively Code Reviewing REST Applications to Avoid Getting Pwned** *Abraham Kang & Dinis Cruz*
12:00	**EMET 4.0 PKI Mitigation** *Neil Sikka*	**Combatting Mac OSX/ iOS Malware with Data Visualization** *Remy Baumgarten*	**HiveMind: Distributed File Storage Using JavaScript Botnets** *Sean Malone*	**This Presentation Will Self-Destruct in 45 Minutes: A Forensic Deep Dive into Self-Destructing Message Apps** *Drea London & Kyle O'Meara*
		A Thorny Piece Of Malware (And Me): The Nastiness of SEH, VFTables & Multi-Threading *Marion Marschalek*		
13:00	**Stepping P3wns: Adventures in Full Spectrum Embedded Exploitation (and defense!)** *Ang Cui & Michael Costello*	**Transcending Cloud Limitations by Obtaining Inner Piece** *Zac Blacher*	**Defending Networks with Incomplete Information: A Machine Learning Approach** *Alexandre Pinto*	**Fast Forensics Using Simple Statistics and Cool Tools** *John Ortiz*
		Utilizing Popular Websites for Malicious Purposes Using RDI *Daniel Chechick & Anat (Fox) Davidi*		
14:00	**EDS: Exploitation Detection System** *Amr Thabet*	**Open Public Sensors, Trend Monitoring and Data Fusion** *Daniel Burroughs*	**Blucat: Netcat For Bluetooth** *Joseph Paul Cohen*	**Forensic Fails - Shift + Delete Won't Help You Here** *Eric Robi & Michael Perklin*
		Collaborative Penetration Testing With Lair *Tom Steele & Dan Kottman*		
15:00	**Conducting Massive Attacks with Open Source Distributed Computing** *Alejandro Caceres*	**PowerPwning: Post-Exploiting By Overpowering PowerShell** *Joe Bialek*	**BYOD PEAP Show** *Josh Yavor*	**Let's Screw with Nmap** *Gregory Pickett*
		Evolving Exploits Through Genetic Algorithms *soen*		
16:00	**Revealing Embedded Fingerprints: Deriving Intelligence from USB Stack Interactions** *Andy Davis*		**The Bluetooth Device Database** *Ryan Holeman*	**C.R.E.A.M. Cache Rules Evidently Ambiguous, Misunderstood** *Jacob Thompson*
17:00	**Closing Ceremonies In Track 1**			

Sekret Notes!

Thank You!

To everyone and all the teams that have made DEF CON 21 possible. Without their hard work, dedication, and time these folks put in the con would not happen. In no particular order:

Great Scott @ Arts & Entertainment would like to thank: Zziks, Mindy, Krisz Klink, ChrisAM, TribalSoul (who make it actually happen). Decor: Zebbler+Co (who make it look good). All the DJs+Musicians (who make it sound good). Fellow DEF- CON staff Ira, Lock, Nikita, Neil, Charel, DT (who keep us from completely losing our sanity). The Rio (who manage to put up with us) + the plethora of other people + attendees I can't squish in here.

Thanks to the NOC team: VideoMan, Mac, #Sparky, effffn, t3ase, Rukbat, Booger, Naifx, Arhawk; and a huge THANKS to Heather, Lockheed and Enki who claim they are "just helping with the transition". These people devote their DEF CON experience to hard work during the DEF CON week and lots of planning throughout the year.

Roamer would like to thank the Vendor Goons: Wiseacre, Wad, AlxRogan, LateNite, Redbeard and Pushpin. Also thanks to Brennan for his work on the Vendor FAQ and Application. And as always shout outs to 303 and Security Tribe.

Agent X would like to thank the Speaker Operations staff for all the long hours, sore feet, missed talks and screwed up laptops. Your work with speakers helps to make DefCon what it is. (I've been told there are talks at Defcon, some day I hope to see one.) The Defcon Speaker Operations staff is: Froggy, Pasties, Tyger, Quadling, pwcrack Shadow, CLI, Mnky, Crash, idontdrivecars, R1sk, bitmonk, Vaedron, Agent X, Notkevin, Pardus, jurlst, goekesmi, Bushy, Code 24, & Gattaca.

Info Booth would like to thank: FAWCR, Melloman, Littlebruzer, Jerel, madstringer, Fran, jaffo, Jenn, Sanchez, ACR0NYM, Project Chatter, Leila T., Mojostico, Littleroo, and William would like to thank all you enigmatic, insatiable, curious, and generally great folks for being a part of DEF CON 21!

Mark Liphardt would like to thank those who've helped for the EFF fundraiser: Doc Who, Dave, Mike, Chris and all those who have participated.

The Swag goons thanks to: secret, Lisal33, OWASPgirl, diami03, Atucom, Daria, GateKeeper, yoshi, gLoBus, veruus, dern, 10rn4, furysama, themikeconnor, Amazon, Scout, bvPredator, Pcfreek14, Dropzone, G-zigg.

The Party Goons: Grifter, Stumper, Gunz, and l3d for keeping the evening events running smoothly and safely. With special thanks to Charel and Nikita for logistical magic. And of course, thanks to all those who submitted to host an "after hours" event, without whom our nights would be a little less l33t.

QM stores is brought to you by Major Malfunction, ETA, Minor Mishap, Wasz, Rick, Red Ace, and countless Juniper Mallets. We would like to thank all the DEF CON attendees and/or the Goons for treating our shit with respect and returning it in the same condition they found it, or at least with a large and tasty beverage to make up for their wrongdoings.

Press: Good hacker news is delivered all over the world thanks to the amazing researchers, VIPs, EFF, DHS, DT, Nico, Dead Addict, Nicole, Dirk, Y0rk, Heather, Kim, Bob, Zelda, Jerry, Lin, Kram, Shawn, Rich, Hoff, Arthur & Hutton.

DEF CON Forums would like to give thanks to Dark Tangent for DEF CON and buying and hosting servers and services to run web content we all use. Thanks to all admins and mods on all web services, disposing of the rubbish and the help they have provided. Mostly, thank-you for tolerating my unfunny jokes. :-) Admins/Mods on pics and forums: Chris, Dark Tangent, ASTCell, Thorn, AlxRogan, BlackBeetle, Neil, Noid, Pyr0, Russ, and added to help with DEF CON Group work on forums: Blakdayz. Also a thank-you to overflow mod support on pics by Nikita and Renderman. Thanks to Dead Addict for the overhaul and cleanup of the TamperEvidentWiki.com and his work as primary admin. Thanks to other supporting Admins: l431l (Neil), and The Dark Tangent. Thanks to Pyr0 for allowing me to make forums for returning contests/events before the RFI, and working with me to help keep forum listings synchronized with reality.

Thanks to Neil for the support in getting the DEF CON 21 web pages synchronized with the forums, and for his custom styles for forums and TamperEvidentWiki. Thanks to Nikita for the updates and hard work to get us those updates.

Security Thanks: Lordy, Evil, Arclight, Amber, b0n3z, BlakDayz, Chosenl, CHS, Converge, Eddy Current, Cyber, Cymike, Dallas, Danozano, dc0de, Deelo, flea, Fox, Fox Captain, Freshman, Gadsden, GM1, Gonzo, Hattori Hanzo, Jake23, JohnD, JustaBill, Kallahar, Krassi, Kruger, Lei, Londo, Machinist, Mattrix, MAXIMUS, noid, Nynex, P33v3, Pappy, Pescador, Pfriedma, Phreck, Priest, Queeg, Quiet, Rik, Salem, Skydog, Synn, Tacitus, TheCaptain, Thyme, Trinity, Vidiot, Wham, WhiteB0rd, dr3t, and Xtacy. The team would also like to send a huge thank you to Lunaslide who is formally retiring after over a decade of service.

Tyler and cstone would like to thank the folks working the desk with us; TW for refining the process after many years of service; and the goons minding the lines for keeping chaos at bay. The registration staff are: Tyler, Matthew, cstone, apebit, phear, crackerjack, 6Q, Soua, Melissa, Zayne, and Aaron.

Blakdayz would like to thank all the DCG POCs that make the DC Groups program the success it is today. Special thanks to russr and converge for the guidance in helping restart the program, and to the DCG Operations staff for dealing with the never ending registration paperwork. The DCG Ops Staff are: salem, ap0k, coreyM, blakbunny, theDNS.

Nikita would like to thank all those above and below for the help and support along the way. Thanks to Sleestak & Tottenkoph for your help as well. Neil & Connor, for giving me the will to survive the sleepness nights. Integgroll, for the lulz & lurve notes. A special thanks to the CFP review board as well. Some of whom are still remaining anonymous, you know who you are. Thank you for your help in reading and providing feedback to the speakers and submitters, and putting up with my animated gifs.

Production would like to thank the many goons working in Production. Dispatch, inhuman reg, photographers and party wranglers! Lock, Doollittle, 1o57, ln, clutch, Zant, Nikita, Neil, MavAntagonist, Tottenkoph, Riggs, Sudo, Voltage Spike, Ahab, noise, Kampf, ElisabethFriday, Rewt, Asmo, cybershaman, Tracie, Viss, Media, Anch, ASTcell, Jolly, Russ, Grifter, Missy, Stumper, Gunz, l3d, Frazier.

Lockheed: Thanks to Riggs for his first-time here helping with Production (n00b!). A huge super-sized thank-you to Zac for all his years as head of operations for DEF CON. Without you, we would never have gotten this far!! Thank you to ALL the Goon staff for their passion and dedication to making this event happen.

LosT: Special thanks to DT, for trusting me yet again. Thanks to eChan, Clutch, Zant, Neil and Kita, and Connorman, the coolest.

DT would like to thank everyone and all the teams that make the con possible. He is constantly amazed and humbled at the energy and commitment of the DEF CON community pulling together each year to throw the best party possible. Thanks to the hard working year round back end DEF CON crew, Neil, Nikita, Charel, Jeff, and new for this year Will for jumping in with both feet and really helping out. Thank you to Jason Scott and his documentary crew for capturing lightening in a bottle and showing the world a bit about what DEF CON is all about. finally a special thank you to Zac for all his years of dedication is helping run DEF CON , and a warm welcome to Lockheed for stepping into his shoes. DT would also like to thank LosT for designing both the badges and the contest around the badges. Has anyone noticed the pattern of electronic, non-electronic badges yet?

A warm welcome to the new photography goons capturing all the madness and mayhem at one of the best parties in the desert. Thanks to ASTcell, Anch, Jolly, Medic, and Viss for trying to be everywhere at the same time.

If you would like to help out or get involved with DEF CON make friends with staff, start a contest, participate in the forums, and I am sure we can find a way for you to contribute! Thank you all, and see you next year.

The Dark Tangent