
DEFCON

WELCOME TO DEF CON 20

Welcome to the 20th anniversary of DEF CON!

When I started this madness long ago I never conceived of doing it for 20 years — yet here we are!

As you would expect this year is designed to be a celebration of 20 years, and we expect the most number of people ever. There is more entertainment, live music, and movie & documentary screenings than in the past. As you have already gathered the badge is our most expensive and sophisticated ever, the music CD of songs donated by artists is a first, and if all goes well the conference CD will actually be a DVD.

We have more bandwidth, more teams competing in Capture the Flag, a new badge puzzle contest, and a faster media server for people to leech off of. Contests have stepped up their game this year, the bands and DJs have been looking forward to it for months, the first FED to be spotted is back, we have the speakers from DEF CON 1 doing turbo talks about what they have been up to all these years, and we have a speaker we have been trying to get for years, the Director of the NSA!

Take my word for it, there is more of everything and it is up to you to find it all out for yourselves. DEF CON 20 is also a year of change, with some people deciding it is best to quit while ahead, to step aside and let new people take over. This continual renewal is what keeps the con fresh, and at the closing ceremonies we will be showing our appreciation to those passing the torch. Hint: Check out Hacker Jeopardy this year, I hear it will be epic.

People are always fascinated with the origins of the con, how it grew from 100+ people that first year to whatever size it is this year. I wanted to get those who knew in the same room speaking to those who wanted to know. That sounds simple, but back in the day there was way more incorrect security information available than was credible and accurate. There was a hunger for what was going on, what worked, and what didn't, that exists to this day. Sure, now we have search engines and a billion security certifications to choose from, but the basic interest remains. The simple formula of good talks, good contests, and good parties allow people to engage in different ways at different times. The con runs 100% on attendees and that has helped us stay focused since the beginning.

A little older but also a little wiser, the people that put on DEF CON are really looking forward to this year. Thanks for making it all possible!

The Dark Tangent

CONTENTS

DEF CON NETWORK

[root@freeside:~] #cat /dev/wifi/ssid/secure

DefCon-SECURE – Type: 802.1x/WPA2

[root@freeside:~] #cat /dev/wifi/ssid/open

DefCon – Type: 802.11b/g [OPEN]

DefConA – Type: 802.11a [OPEN]

Once again, we have 100 megabaps of Internet bandwidth for you. We have WiFi throughout the entire Rio convention center. We continue to provide both a "secure" and "free range" wireless network. The Secure network provides you access to internal infrastructure/servers and to the Internet – that's it! No client-to-client connections (so less chance of finding goatse the hard way).

Shout-outs to the NOC staff who keep things running every year: Lockheed, Heather, Mac, effffn, Rukbat, Videoman, Enki, Mac, #Sparky, and t3ase. This year we have interns – Jared, Justin, and Erik!

Let us know how the network's working – noc@defconnetworking.org.

Check throughout con for stats & wrap-up at http://www.defconnetworking.org/

DEF CON TV

We continue to send the DEF CON talks direct to your hotel room! We're also going to try to do a multicast stream so you can watch from your laptop/tablet. We have a new crew to help make DCTV ultra kick-ass this year! Check out http://DCTV.defcon.org for up to date on-site info and program options.

For information or requests email dctv@defconnetworking.org

THE BADGE

My goal last year with the badges was to foster communication amongst attendees. There was phenomenal participation in the 'mysteries' tied to the badges and the conference, and I hope that everyone had fun. Helping build the hacker global community is a great side benefit that I always hope I can be a part of.

This year I decided to try and combine the awesomeness of the legacy of electronic badges Joe had set, with the well-received badge challenge from last year, but with a twist - rather than handing you a purposefully designed circuit for hacking, I've tried to give you a development platform. A platform that hopefully you'll take home and use.

I went with the Propeller ucontroller for a number of reasons. It's no secret that I used to work for Parallax, and as such have experience with their chips. All of the software for programming the Propeller is free, and there's quite a variety; C, ASM, SPIN- and if you're feeling nostalgic a Z80 emulator and a C64 emulator in the works as well. The chip itself has 8 32-bit processors, so the pains involving interrupts and timeslicing are non-issues. Fabrication of the badge was all done in the US this year as well, to avoid all the import issues DEF CON has encountered in the past.

The VGA and PS/2 connectors were left off of the build intentionally, so that the badge is lighter while you wear it at con- but everyone got them as encouragement- either to visit the Hardware Hacking Village and attach them here, or to solder on at home. Now you have an excuse to finally learn to solder if you haven't before. Drop by the HHV, they'll teach you. You can power the badge via the USB connection or batteries, either one.

The USB connector can be used with a serial terminal (some output may already be there on boot, hint hint), and I've broken out I/O pins (on the top) for your hacking pleasure.

The badge challenge this year is actually two challenges in one- the 'crypto-mystery' game, AND hardware hacking/development/modification. Teams completing the game will require a 'modification' as part of their 'conclusion', and those wishing to submit a hardware mod need to do so with a team with the appropriate 'codeword' discovered in the game. Now you have to talk to each other ;)

Hints for the game will be forthcoming from my twitter account (#1o57), but here's your first one:

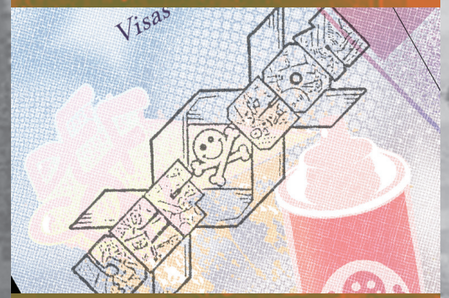
www.defcon.org/1057/??????????

Happy 20th DEF CON. Thanks DT.

-Ryan "LostboY" Clarke

GET STAMPED!

DEF CON is joining the ranks of cool Hacker Spaces world-wide by offering not only to stamp your Hacker Passport with an entry stamp for DEF CON 20, but also by offering our own Passport Book.



The idea is simple, and follows in the path that Mitch Altman and Matthew Borgatti started over at http://HAR.MS/HACKERPASS where you download and print out your own passport then take it to various hackerspaces as you travel the universe. (hackerspaces.org for a great list) When you visit a participating space they stamp your passport if you ask.

DEF CON will be making stamps for all future years as well as giving away our own pdf of a template passport, and for those of you not so hot with paper and staples we will have one for sale pre-made in the vendor area.

Get yourself stamped at the info booth or the human reg area!

MEDIA20 SERVER

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

Point your browser at ftp://dc20-media.defcon.org or we bDAV to port 5005!

Last year it was a Synology 411slim NAS server that was pumping out 160 Mbps, as fast as its little low power processor could go. The newer hardware for this year should lead to faster downloads.

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!

MEDIA.DEFCON.ORG

Hacking is the future. Having the skills to control your own destiny, to bend the crazy information stream to your will, and to protect yourself from digital harm will only become more crucial as time goes forward.

But hacking is also the past. There are amazing things to be learned from the story of how we got to where we are. There's a wealth of actionable insight available to you in hacker lore and legend.

DEF CON is trying to do its part to keep that information available and free, via the DEF CON media server. In it, we archive as much as we can of DEF CON's past content, and whatever we can scare up from other sources and host (with all the appropriate persmissions firmly in place, natch.) Want to learn how Aaron Higbee and Chris Davis turned an old DreamCast into a phone-home device? It's there in the archives for DC 10. Feel like reliving the insane rockstar-ninja-pimp introduction of Back Orifice to the world at DEF CON 7? We have it (Spoiler: there are pyrotechnics and profoundly misplaced telco equipment.) Even if you're just doing independent research on the effects of free beer on higher cognitive function — we have a couple episodes of Hacker Jeopardy just for you. [Ed. note: Winn, never shave. Shaving ruined Trebek.] There are even a few hacker documentaries archived there. Visit, learn, marvel and be entertained.

https://media.defcon.org/

The story of how ordinary hackers tilted the paradigm of technology and power ever so slightly closer to the little guy is important, maybe one of the most important stories of our time. We have some of the pieces, but we're hoping to assemble more of the puzzle for posterity.

That's where you come in. If you have cool, hacker-related infoz, in any digital format, that you'd like to see in the archive and shared with the world, send us an email at dt@defcon.org.

BLACK AND WHITE

FRIDAY BLACK BALL

+BAND

MC frontalot

and

MINIBOSSES

alongside

RECOGNIZE - THE GOON BAND

REGENERATOR

KRISZ KLINK

CY-FI

SAILOR GLOOM

Friday, 21:00-04:00 in Track 1 (Rio Pavilion 8-11)

SATURDAY WHITE BALL

the crystal method

and

ELITE FORCE

alongside

ZEBBLER ENCANTI EXPERIENCE

MISS DJ JACKALOPE

MITCH MITCHEM

GREAT SCOTT

Saturday, 21:00-04:00 in Track 1 (Rio Pavilion 8-11)

CHILLOUT AND POOLSIDE

THURSDAY POOLSIDE

Mochipet

and

MC frontalot

alongside

DUAL CORE

DALE CHASE

OBJECT D

YTCRACKER

SAINT VII

DR.RAID

AN HOBBES

Thursday, 19:00-03:00 at the Pool

FRIDAY POOLSIDE

PHREAKOCIUS

RENE

RYAN GATESMAN

ELECTRIC

SIGMA STARR

DJ%27

ROBB WISE & TAD TIMOTHY

Friday, 19:00-03:00 at the Pool

SUNDAY POOLSIDE

PROJECT MAYHEM

YTCRACKER (DJ SET?!)

{ ZACK FASEL & KEITH MYERS (BATTLE ROYALE!) }

VJ Q. ALBA

MITCH MITCHEM

ALBA T. ROSS

KAMPF

Sunday, 19:00-03:00 at the Pool

CHILLOUT

NOP

KAMPF

ROBB WISE & TAD TIMOTHY

PHREAKOCIOUS

24hrs in Miranda

CONTESTS

Beverage Cooling Contraption Contest

Saturday at 13:00 on the Miranda Patio

The fact is that many of the beverages we consume are just plain better when they are chilled. Hackers are always making tools to make their lives better. Why not tools that chill beverages?

Let's cool some beverages! Sure we know how to drink em, but how fast and accurately do you think you can chill them?? .

Teams will pit their creativity and ingenuity to the test. Their contraptions will be tasked with taking an outside temperature beverage (probably 83+ degrees Fahrenheit depending on the Las Vegas sun) and chilling it to exactly 42 degrees Fahrenheit this year. There are bonuses for per beverage chilled and penalties for missing the target temperature. After adding both penalties and bonuses, the fastest time wins!

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

Come and see the technological contraption wonders that chill glorious beverages.

Some teams do it for prizes. Some teams do it for glory. Some teams do it for SCIENCE!

Everyone at this contest watching or competing is sure to have a great time. So come on down to the Miranda Patio on Saturday at 1:00pm.

Official Rules and team sign ups are at the DEF CON Forums contest area.

DC20: [Official / Unofficial] [Parties / Social Gatherings / Events / Contests] "Beverage" Cooling Contraption Contest

Black Bag

13:00 – 17:00 In the Contest Area

At past DEF CONs Deviant Ollam and his company, The CORE Group, featured the Gringo Warrior lockpicking contest. In that scenario-based escape game, participants had to "break out" of a virtual prison cell and escape kidnappers in a quest for freedom. Many came, many succeeded, all had a good time. In this latest contest designed and built by The CORE Group, you will use similar skills and cunning... but with the aim of getting IN and then getting BACK OUT from your target building.

Black Bag is a team-based physical penetration event. Three-person teams will be tasked with infiltrating the offices of a shadowy super-criminal with the goal of uncovering details of his plans and associates. Using genuine tools and equipment used in the field, you will have to compromise physical locks, disable surveillance systems, copy keys, access and photograph documents, gather information from computer systems, unlock smartphones, and even attempt to remove a desktop computer from an office WITHOUT powering it off.

Pulses will race... brows will sweat... sparks may even fly! In the end, we will see how many objectives you and your teammates can accomplish in ten short minutes without being caught or leaving any evidence behind!

CTP: Capture the Packet

09:00-19:00 in the Contest Area

CAPTURE THE PACKET
Network Analysis & Forensics Skills Assessment

Capture the Packet is in its third year, now a Black Badge Event !. CTP Capture the Packet is a one hour "live traffic analysis game". Here you will see no static PCAPs, it's like being on the wild, wild west internet. You are competing against some of the best traffic and forensic analysts to use your Packet FU – and analysis skills to beat your opponent and prove you can "Capture The Packet".

Contestants will monitor the hostile CTP network, use traffic analysis skills to look for clues, solve puzzles, trivia, and complex analysis questions – Answer them correctly and receive points, answer them incorrectly and you lose points. The high score in that round and move the Final round on Saturday evening where you have a chance to complete for some really great prizes, including the DEF CON "Black Badge".

Register online at "CaptureThePacket.Com" or at the CTP table here at the conference, provided space is available. Check out our facebook page for static pcaps to help build your skills and give you the confidence to register to compete at DEF CON 20.

Crack Me If You Can

48 hours straight. 23:59pm Thursday July 26th – > 23:59 pm Sat Jul 28th

Teams have 48 hours to crack as many passwords as possible. The hashes are provided (and generated) by the KoreLogic team to range from simple to "challenging". The teams are required to crack, recognize patterns, innovate solutions to crack more passwords, and then repeat the process over and over again. The trick is winning is the best combination of team work, good wordlists, rules, hardware, and being able to use PGP/GPG email properly. The contest is designed so that even password cracking beginners can have fun and crack lots of passwords. But at the same time, the advanced teams of the world's best password crackers will be burning the midnight oil to crack as many hashes as humanly possible in the short amount of time. This is our 3rd year running the contest, and we have a bunch of new tricks up our sleeves for "challenges" that teams will try to win. TrueCrypt encryption? Sure! MD5s ? of course! NTLMs galore. ZIP files? RAR Files? SHA256? Hash formats unsupported by any tool – but still used in the "wild" ? Expect it ;) Fire up your GPU cards – ramp up your EC2 clusters. Your college doesn't need that big ol' cluster over a random weekend in July does it? Use that! The teams are fighting for $1,000 dollars in cash (split between 1st, 2nd and 3rd place). All teams must have at least 1 member onsite at DEF CON.

Crash and Compile

20:00-24:00

A programming contest crossed with a drinking game. What can possibly go wrong?

Dark Tangent's Tamper Evident Contest

Noon Friday to 2pm Sunday In the Contest Area

The world is full of 'tamper-proof' packaging. You're expected to trust it, but how strong are those measures, really? This is a contest about defeating these physical measures in a documentable, elegant fashion that leaves no trace of your attack. You can enter alone or with a team, and you can even enter the 'Unlimited 'class that allows you to use any tools or gear you can get your hands on.

Lost @ Def Con Mystery Challenge

All Con

The LosT@DEF CON Mystery Challenge comes out of retirement for DEF CON 20. Although registration takes place prior to con, DEF CON 101 offers unique opportunities for con newcomers to be placed on existing teams. Teams never have any foreknowledge regarding the challenge each year, only knowledge of past challenges provides any possibility of preparation. Past challenges have incorporated elements of social engineering, networking, electronics, mathematics, physics, physical security, linguistics, pop culture, lockpicking, cryptology, esoteric knowledge, reverse engineering, riddle/puzzle solving, costuming, roleplaying, bookbinding, and what ever else LostboY/1o57 (Ryan Clarke) can come up

with that year. The goal is to have something fun for everyone participating, and creating new friendships (and enemies?) while competing in one of the most challenging Defcontests (trials of pain?) . Originally created as an interesting way to give free hardware to interested HUMAN attendees, teams often leave the contest with a sense of accomplishment and free hardware. Winners of the mC are generally rewarded with a DEF CON black Uber badge. Hackers of the world unite

Pbzr ba thlf, EBG guvegrra? Lbh jvfu vg jnf gung rnfl. Jung qb lbh guvax guvf vf, gur onqtr pbagrfg?

Open CTF

In the Contest Area

Open CTF is a Capture the Flag contest that is open to any and all attendees. This year's game features a new style of competition that combines both Jeopardy-Board and Attack/Defend styles into one high-intensity game. Unlike previous years and other contests, this year's OpenCTF will be played as a single-elimination tournament, with multiple rounds spread out over three days. The best will win, but not at the cost of spending their entire DEF CON 20 experience huddled over a laptop in a dark room listening to repetitive electronic music and munching on magic pills.

Project 2

Friday 09:00-20:00(ish) Saturday 09:00-20:00(ish) Sunday 09:00-14:00 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.

REBOOT ARG

24/7

Players need to watch the trailer for REBOOT at www.rebootfilm.com, and see what they can find. When Players finds anything they think is an Easter egg or a "key" to the next level, they need to send a direct message to REBOOT on Twitter (@reboot_film) for confirmation. We will respond letting players know if they have found a clue or if they have reached a new Level. Note: you must follow us on Twitter in order to send us a direct message. How players get points? Points: Level 1 = 500 (Players get these points just for playing the game) Level 2= 1,000 Level 3 = 1,500 Level 4 = 2,000 Level 5 = 2,500 ...and so on. How many levels are there? Hehe... we can't tell you that. :) Clues or hidden message that Players find (and are confirmed by REBOOT) are worth: 100 points each. What Players win? Our Overall Champion and #1 Player will win a free HD download of REBOOT upon release; the Official Soundtrack signed by the composer, and an 11x17 Poster of the film signed by the writer/director. The Top 5 players will win a free HD download of REBOOT upon release. The Top 10 players will win a free digital download of the Official Soundtrack for REBOOT. Good

CONTESTS

luck to everyone and thank you for playing! We hope you enjoy the game.

Scavenger Hunt at DEF CON

Friday 10:00 to 18:00, Saturday 10:00 to 18:00, Sunday 10:00 to 13:00 In the Contest area

Scavenger Hunt is a contest of will, creativity, smarts and chutzpah as teams search for unusual items and complete insane stunts. This year will be our 15th year anniversary! To celebrate we have some insane surprises! With prizes provided by ThinkGeek.com, as well as items from each and every vendor in your vendor room, the rewards will be amazing! Be sure to follow us on Twitter @ defconscavhunt and on Facebook at https://www.facebook.com/defconscavhunt and be sure to enjoy this discount while shopping at http://www.thinkgeek.com using code DEFCON12, good for $10 off $60+ orders from 7/26/12 to 11:59pm ET 8/5/12

The Schmooze Strikes Back - SECTF 3 (Social Engineering Capture the Flag 3)

Friday-Sunday in Palma E-F

Returning to DEF CON 20, the Crew at Social-Engineer.org is challenging you. We are inviting those of you who think you can use ethical social engineering skills to stretch your limits as a social engineer. A unique blend of information gathering, planning and attack vector execution will challenge the very core of every participant. This will be a different SE challenge as our focus is not on who can "get" the target the worst, but a true display of SE talents.

The Schemaverse DEF CON Tournament

Thursday – Saturday 09:00-19:00 and Sunday 09:00-12:00

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!

Wall of Sheep

Hours of Operation – 09:00 – 19:00 in the Contest Area

The Wall of Sheep is an interactive look at what could happen to you if you let your guard down when connecting to any public network. The Wall of Sheep passively monitors the DEF CON network looking for traffic from users utilizing insecure protocols. The Wall of Sheep will be hosting several BackTrack 5 – Network Sniffing 101, using Wireshark, EtterCap, Dsniff and other traffic analyzers. We will also be hosting an Advanced Traffic Analysis and Password Sniffing and many other Classes through-out the conference – check the schedule at the Wall of Sheep for dates and times. Come be part of history and capture traffic at the "Wall of Sheep" for yourself. New this year is the "Wifi Sheep Hunt" contest, visit the Wall of Sheep for the instructions and prize details, you will want to hunt those sheep down.

25,000C Hacker Pyramid

Fri-Sat at 20:00 in Track 3

Back for DEF CON 20 – The 25,000¢ Hacker Pyramid!!! Come and be a lucky audience member who will participate with a DEF CON Celebrity in a fast paced game of Pyramid! It may be the last Dick Clark property to be Seacrested... so we're bringing it to you FIRST! Every contestant has a chance at the FABULOUS PRIZES—all the way up to the GRAND PRIZE of 25,000¢!!!!!!!

BroCTF

10:00-22:00 Fri-Sat, 10:00-? Sunday in the Contest Area

Sup Broseph!?

I was playing this sick game of ultimate today with one of the other startups at our co-working space. They were burning super hard after we kicked their ass and started talking mad shit. One of the dudes starts talking shit about my programming chops and I was all like, "Come at me, bro!" Then he was all like, "Naw Kimbro Slice, we gotta handle this right. We're having a brodown!" They told me about this contest out in Vegas called BroCTF. At first I thought it was some kind of sweet mashup of dirt biking and capture the flag but apparently it's this totally chill competition for hackers and brogrammers.

The contest is supposed to be at this epic hacker meetup called DEF CON which is having it's 20th Anniversary this year. I was thinking we grab some more bros, road trip out to vegas, and show these scrubs how to rage like real brogrammers. I hear they're gonna be bumping some hardcore brostep all weekend and have some totally sweet challenges this year. The game is suppossed to run Fri and Sat 10:00-10:00 and most of the day on Sunday. Should give us plenty of time to show these fauxbros what's up and still slam some jager bombs at the clubs!

DEF CON Beard and Moustache Championship

In the Contest Area

Due to the growing number of awesome beards at DEF CON and the (popularity?) of the shitshow that is beardsmanship, it's time that folks were recognized for letting their unix beards fly.

Network Forensics Puzzle Contest

In the Contest Area

The Network Forensics Puzzle Contest is a challenging mystery requiring contestants to forensically analyze packet captures (and more!) to uncover an evil plot.

Spot the Fed

Of course you know they walk among us, these badge-wielding, security-clearance having dot gov types. You've got the warning signs down, from the haircut to the tucked in shirt, from the shifty eyes to the sun-kissed skin. There's really only a few questions left. Do you have the stones to make your suspicions public? Do you have a line of questioning that will force your quarry's hand? Can Priest make your target crack and win you the rare and coveted "I Spotted the Fed" t-shirt?

To get in the game, you need to alert Priest of your discovery. He can be reached in person, via the Goon team, or through the info booth. If you get Priest and point the FED out to him, and you have the stones to do it, get the FED up on stage for a crowd vote on whether they quality or not!

As always, we are not looking for "pseudo-feds." There are more than enough gun and badge types with arrest powers for this contest, so civilian contractors and off-duty military don't qualify.

Spotted Feds: In return for the good-natured ribbing you will receive from the con attendees, those Federales whose covers have been blown receive the equally treasured "I Am the Fed" shirt. Let the soft, fluffy cotton blend soothe all the hurt away.

Un-spotted Feds: Are you a Fed so crafty you remained unspotted? Did you get the DC pallor down so well that we think you're one of us? Rumor has it that contacting Dark Tangent directly (I know, good luck) in some quiet place will get you on the mailing list for your own "I Am the Fed" shirt. If you have schwag to trade you need to find Major Malfunction, DT's official Avatar for trading goods. Of course, this might get you spotted, so be stealthy in your movements. Major Malfunction also has access to the list - but if you're as good as you think you are you can definitely find DT.

The Official BloodKode Challenge

10:00- 17:00 Friday and Saturday in Palma G

Please join us for BloodKode 2.0 Last year the hacker community did what it does best & came together to help one of it's own. This year we ask for the community to come together to help everyone! The BloodKode is more than donating blood in honor of a friend. It's not about the random drawing of cool swag you get when you donate. Heck it's not even about making your drinking tab cheaper (You know what we mean) It's just about helping out someone who you will never meet and giving them the gift of life! No Mohawks this year but Awkward Hugs will be given & the silent thanks of the person you helped & their loved ones! So donate early & often.....err scratch that last part! Just remember the blood of hackers run through your veins time to share that gift with the world!

DEF CON Short Story Contest!

For the past few years I have been running a short story contest on the DEF CON Forums (https://forum.defcon.org/). These stories are tune with our community, I wanted stories about hackers, hacking, science, technology, nerdy things, geeky things, zombie things. This year I wanted contestants to tie their stories in with the conference itself. So if they wrote about zombies chasing a group of young folk, they better be at our con, staving off a hoard of the undead while building a lab to find a cure for the T Virus. (Believe it or not, someone actually wrote a similar premise) I've included the past 3 years worth of short stories on the conference DVD for you to read. You will find no hair tussling in the breeze, bodice ripping, stories that you can find in the romance bin. No matter how you dress it up with tech, it's not worth it to me read nerd porn unless it's a tiger direct or fry's circular. You can follow me on twitter at Niki7a if you want to, If this seems like an exciting method of communication to you.

New for this year, the DEF CON Forum meet proposed a short story reading and a sort of meet the author event, so be sure to visit the DEF CON Forum Meet 19:00 Saturday in Palma G&H and check it out!

Here are the winners for this year!! Thanks everyone who submitted!

First Place - A Silent, Private Place, by Davien, won 2 human badges!

Second Place -DEF CON Unbound, by John McNabb, won 1 human badge!

People's Choice - DEF CON Unbound, by John McNabb, won another human badge!

Honorable Mention- DEF CON - The Beginning of the End, by Siobhan Morrison

DC 20 CAPTURE THE FLAG

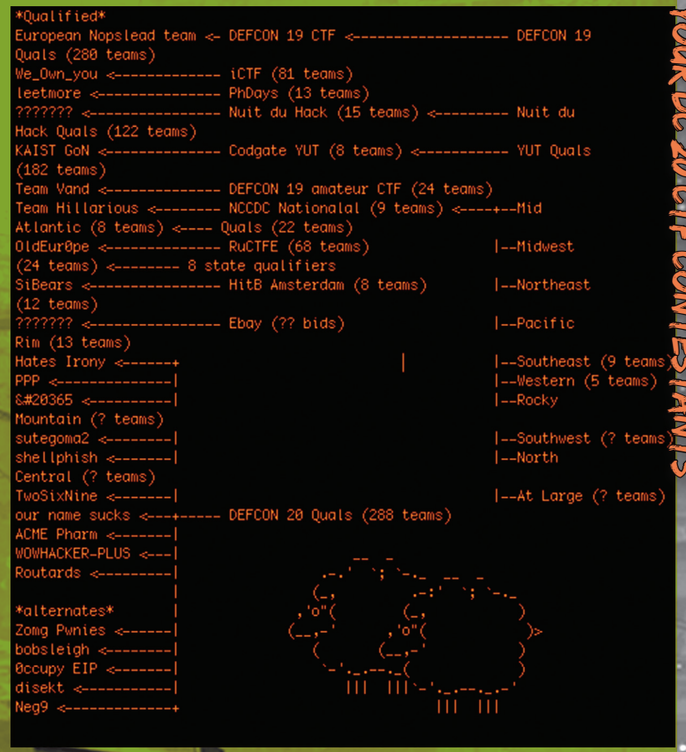
Once again, the DEF CON Official CTF contest is the biggest it's ever been. Hundreds of teams around the world have fought their way through a brutal bracket system in order to get the coveted invitation to play in the big show at DEF CON 20. The 20 gangs of network Highlanders who made it here are probably at it as you read this. The contest goes on until the bitter end of the con, leaving just enough time to finish the scoring and get everyone into the closing ceremonies.

The twenty teams competing the this years contest, Binjitsu IV, come to us through quite a few different channels. 10 teams got their spot by dominating the open qualification round hosted by Binjitsu IV's organizer DDTEK.

We also invited teams who showed their skill by winning other respected CTFand hacking contests from around the world.

And finally, in a new twist, the final slot is being auctioned on Ebay. Team "cashcows" will get their slot by winning the auction, with proceeds going to a combination of contest costs and charity.

It's hard to overestimate the level of difficulty here. The contests get more difficult every year, and the set of skills a team must display to win gets wider as well. Every single team here deserves your admiration. DEF CON and DDTEK wish the best of luck to all of them.



YOUR DC 20 CTF CONTESTANTS

BINJITSU IV POWERED BY DDTEK

Scoring a CTFis a challenging proposition.

In order to become a master of binjitsu, it is essential to understand how you will be measured.

Services constitute the heart of the CTF game. Each team must attack and defend identically configured servers, each running some number of custom services. The idea is to analyze the custom services for vulnerabilities and to develop both an attack and a defense strategy for each service. By exploiting a service an attacker gains access to privileged information which is generally referred to as a key (aka flag, aka token). Keys may be readable (steal information), writable (corrupt information), or both. Teams demonstrate that they have stolen information by turning stolen keys into a key submission server. Teams demonstrate that they can deface a service by overwriting keys with a replacement key unique to the attacker. For both of these activities, teams are awarded points. In order to keep things interesting, keys are periodically updated by the contest organizers, allowing teams to demonstrate that they can maintain continued access to their victim's data through submission or corruption of the new key values. Additionally the period during which teams may submit stolen keys is finite (for example within 30 minutes following the steal) in order to reduce the effects of key hoarding (displayed score not representative of actual score) and key sharing (where teams obtain keys by trading with other teams rather than via attacking other teams).

Ratherthan simply awarding a point perstolen oroverwritten key, the scoring system treats keys as commodities (such as diamonds). The following factors are taken into account when deriving a team's overall score:

1. The more keys that are stolen/overwritten for a particular service, the less each key is worth.
2. Teams earn more points for demonstrating diversity of attack across a given service. In other words, teams can score points for attacking the weakest defender, but they can earn far more points by demonstrating that they can attack across all other teams as well.
3. The longer a team's attacks go unnoticed, the longer that a team remains the sole possessor of an 0-day, the more points a team can accrue for a given service (effectively cornering the market on that commodity)

Teams are awarded points as follows:

1. For a given service up to 1800 points are available for distribution to the teams. 900 points for reading keys from their 9 opponents and 900 points for overwriting keys of their 9 opponents.
2. For a given attacker, a given victim V, and a given service S, the attacker's partial score for the stealing keys from the service is their percentage (0-100) of all keys stolen from V via service S.
3. For a given service S, an attacker's score for service S is the sum of the their partial scores (across all of the other teams) for that service.
4. A team's overall raw score is the sum of its scores across all services in the game, minus defensive penalties for any of their keys stolen by other teams.
5. A team's raw score is then multiplied by a measure of the availability of the team's services for the duration of the game. Note that availability does not imply the service is unexploitable, so the team may not in fact be defending the service.

One example of a partial score awards a team 100 points if they are the only team to steal keys for service S from victim V, even if the attacker steals only one key. Thus this is a very valuable key. In another example team 1 may have stolen 400 keys, team 2 300 keys, team 3 200 keys, and team 4 100 keys from service S on victim V. In this second case, the teams are awarded 40, 30, 20, and 10 points respectively. In this case, individual keys are worth less because keys for this service are common.

An interesting effect that may be observed under this scoring system is that a team's score may actually decrease from time to time. For example, the first team to submit a key for a service/victim will have the one and only key submitted and therefore a partial score of 100 (percent) for that service. If a second team submits a key for the same service/victim each team's partial score will now be 50 points and the first team will see a decrease in their score owing to the fact that their 0-day is no longer as valuable as it once was. On the other hand if the first team manages to capture 99 keys before the second team submits their first key, the first team will see their score drop almost imperceptibly from 100 to 99 while the second team's score will be only 1. This situation reflects the first team's early entry into the market for these keys and their near monopoly on these keys.

Those familiar with the "breakthrough" system of past CTFs, may note that there is no mention of breakthroughs in the description above. We feel that this scoring system rewards 0-day when 0-day is used effectively to build one's hoard of keys ahead of any other team developing their own version of the same exploit. Further this system allows teams to delay the use of their 0-day in order to keep the number of keys in play to a minimum with the associated risk that another team will beat them to the punch. Thus, in addition to testing a team's offensive and defensive skills, this scoring system attempts to make teams consider the strategy of how, when, and where to make use of their 0-day. Additionally it places increased emphasis on keeping exploits stealthy.

Stop by the CTF room and talk to a DDTEK representative for more details on the scoring system and displays you will see during the contest.

~ur CTF cr3w

EVENTS

Be The Match - National Marrow Donor Registry Drive

Fri – Sun, 09:00-18:00 in the Contest Area

Back for its third year! Take part of the coolest "Bio-Hack" around... register with "Be the Match" at DEF CON, and take the first step to become a Bone Marrow Donor, by signing up on the Be the Match donor registry.

DEF CON 20 Forum Meet

Friday at 21:00 in Palma G-H

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.

It's the place to meet other likeminded individuals in a casual easy going atmosphere, no loud music or flashing lights. A place conducive to just talking and having good conversations.

The "Forum Meet" is not meant to be a "Destination" it is a "starting point" a place to meet people with similar interests and then go explore all that DEF CON in Vegas has to offer!

Hacker Karaoke

Thursday: 21:00-02:00, Friday or Saturday (TBD): 21:00-02:00 in Brasilia 1

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 16:30-22:00, at Sunset Park

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 to the BBQ site. Many of the organizers can be found at the BBQ pits.

Queercon

Social Mixer: Friday & Saturday - 16:00 @ I-Bar

Party: Friday - 20:00 @ Brasilia 3

Queercon is back and celebrating its 9th year!

Looking for a safe place you can relax and meet other LGBT hackers?

Join us Friday and Saturday starting at 4PM for the Queercon Mixer at I-Bar. It's a great time to drink, socialize and meet other people.

Friday at 10PM Queercon kicks into high gear with the hottest DJs at Defcon. Queercon is open to all LGBT hackers and friends. No bad attitudes and no invitations needed - come as you are. You are beautiful and we love you!

Stay up to date with all queercon activities at queercon.org

IOActive Freakshow

Saturday night at the pool

Representative of both the DEF CON community and the values of IOActive's own principles, the Freakshow is always inclusive, fun, and constantly pushing the boundaries of what is new and exciting.

The Freakshow has humble beginnings. Launched in 2007 as an opportunity to utilize some extra space and give back to the information-security community, we expected 500 people to attend, and were astounded by 1000 party-goers. Last year's Freakshow saw record attendance of over 4,000 people and included live music, fire dancers and all around good spirit. This year DEF CON 20 is posed to be the biggest and most electrifying year in the history of the conference and the Freakshow is no different. Celebrating our 5th anniversary,we look forward to this year being bigger, better and freakier than ever before!

VILLAGES

Lockpick Village

10:00 – 18:00 daily in Tropical C,D,G,H

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 Tropical A

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 1

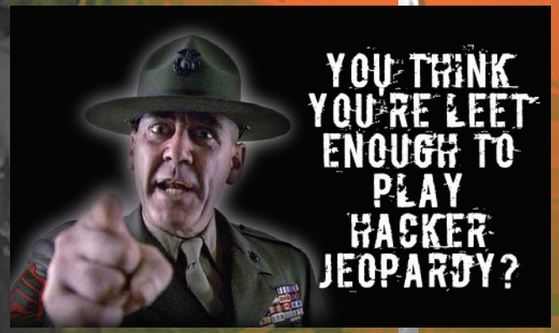
Many Defcons ago LostboY (aka 1o57) walked from one end of the DEF CON conference spaces to the other, shouting the question, "Who wants to learn how to build a simple robot?" Eventually a large group wound up sitting on the floor in the contest area building and programming robots. Inspired by that 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.

HACKER JEOPARDY

In the beginning DT created DEF CON The First. And the con was formless and empty of games, and darkness was rolling in the deep.



And Winn said, "You need a contest." DT said, "Like what?" Winn said, "Shit, how about Hacker Jeopardy?"

And DT said, "Let there be Hacker Jeopardy," and the next con there was. And there was evening, and there was morning — the first DEF CON contest.

And Winn said, "Let there be alcohol," and there was alcohol in copious amounts. And the beer did flow and the contestants did guzzle and burp. And each beer was worthy of 100 points. And there was evening, and there was morning — the first DEF CON contest with free beer. And Winn said, "Let there be breasts," and there were. And the bare breasts pranced around the stage as a reward for Double Jeopardy, and Winn called them "Bad" and "Kitty." And there was evening, and there was morning — the first DEF CON contest with free beer and nudity.And Winn said to DT, "Let there be a black badge," and there was. And DT added leather jackets to the rewards. And there was evening, and there was morning — the first DEF CON contest with free beer, nudity, and a black badge.

And Winn said, "What the fuck ... Let there be humiliation," and there was. And Winn heaped abuse and humiliation on every wrong answer, and brought forth special humiliation for every wrong Double Jeopardy answer, which denieth the people a glimpse of the breasts waiting to be bared on stage. And there was evening, and there was morning — the first DEF CON contest with free beer, nudity, a black badge, and humiliation.

And Winn looked on all that he had created, and saw that it was good. And on the twentieth year, Winn said to DT, "What the fuck hast I wrought...?"

And all the people of the twentieth year were invited to find out what the fuck was wrought.

THE ONE. THE ORIGINAL. THE OLDEST & ONLY
DEFCON EVENT WITH REAL SKIN IN THE GAME.

DON'T FUCK IT UP.

HACKER JEOPARDY

WINN G MARK VANNA VINYL FIZZGIG BEER BETTY ET AL.

IF YOU'RE REALLY LUCKY, MISS KITTY JUST MIGHT SCHOOL YOU!

FRIDAY 7/27/2012 & SATURDAY 7/28/2012 • 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

DEFCON KIDS II

DEFCON Kids is a not-for-profit teaching kids around the world how to love being white-hat hackers. **http://www.defconkids.org**

DAY 1 FRIDAY

	Classroom in Belize	Workstations in Antonio's Ristorante	Contests in Antonio's Ristorante	Field Trips at DEF CON 20
10:00 - 11:00	Meet Top Secret Keynote General Alexander	Code Breaking Museum NSA **10:00 - 18:00**	Hoff's NSA Crypto Challenge	Welcome and The Making of the Badge Dark Tangent and L0st
11:00 - 12:00	The Wall of Lambs FS and cedoxx	SnapCircuits beaker and cl0ver **11:00 - 18:00**	Hacker Board Games	Can you track me now? Government and corporate surveillance of mobile geo-location data. Christopher Soghoian
12:00 - 13:00	Geek Out! beaker and cl0ver	Wall of Lambs FS and cedoxx	The Lambs & The Wolves	Top Secret Keynote General Alexander
13:00 - 14:00	Welcome to DEF CON 20 Dark Tangent	Go Eat!	Go Eat!	The Making of DEF CON 20 DEF CON Goons
14:00 - 15:00	DEF CON Badge Secrets L0st	Find a Zero-Day CyFi	CyFi Zero Day Contest **14:00 - END**	Changing the security paradigm... Shawn Henry
15:00 - 16:00	Hacking Hotels and the Law Major Malfunction and Max	Lockpicking Deviant	DEF CON Badge Secrets **15:00 - END**	DEF CON Badge Secrets L0st
16:00 - 17:00	Taking Open Source Drones Mainstream Chris Anderson	Hacking Hotels and the Law Major Malfunction and Max	Lockpicking Race	Safes and Containers Marc Weber Tobias
17:00 - 18:00	How to Use Social Engineering Chris Hadnagy	Q&A on Drones and 3D Printing Chris Anderson	Hacker Board Games	The Real Hustle Paul Wilson
18:00 - 19:00	Go Eat!	Go Eat!	Capture the Flag **18:00 - END**	Go Eat! All American Bar & Grill
19:00 - 21:00	Movie War Games - PG	Movie Sneakers - PG-13	Movie Sneakers - PG-13	Go Eat! All American Bar & Grill

DAY 2 SATURDAY

	Classroom in Belize	Workstations in Antonio's Ristorante	Contests in Antonio's Ristorante	Field Trips at DEF CON 20
10:00 - 11:00	Hacking Your School's Network Cory Doctorow	Code Breaking Museum NSA **10:00 - 18:00**	DoD Crime Scene Investigation **10:00 - 18:00**	World War 3.0 - The battle for the Internet between the forces of Chaos & Control Michael Joseph Gross, Vanity Fair
11:00 - 12:00	Lockpicking Deviant	SnapCircuits beaker and cl0ver **11:00 - 18:00**	Hoff's NSA Crypto Challenge	Hacking Humanity: Human Augmentation and You Christian Quaddi Dameff
12:00 - 13:00	Weaponizing Mobile Marcus & Erran Carey	Wall of Lambs FS	The Lambs & The Wolves	DIY Electric Car David Brown
13:00 - 14:00	Go Eat!	Go Eat!	Go Eat!	Go Eat!
14:00 - 15:00	Practical Privacy Tips Moxie Marlinspike	DEFCON Kids TV Production DH & Goodson **14:00 - 18:00**	Chaos & Control	Fed Panel Priest
15:00 - 16:00	Hardware Hacking and Soldering Joe Grand	Coding with Scratch beaker and A1ex	Hacker Board Games	Bigger Monster, Weaker Chains: The NSA and the Constitution ACLU
16:00 - 17:00	Hardware Hacking and Soldering cont'd Joe Grand	3D Printing with Frosting beaker and A1ex	Coding with Scratch	Hacker + Airplanes = No good can come of this RenderMan
17:00 - 18:00	The Feds Jim Christy	Meet the Feds Jim Christy	Spot the Fed	Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit Dustin Hoffman
18:00 - 19:00	Go Eat!	Go Eat!	Go Eat!	Go Eat! Martorano's
19:00 - 21:00	Movie Hackers - PG-13	Movie The Net - PG-13	Movie The Net - PG-13	Go Eat! Martorano's

DAY 3 SUNDAY

	Classroom in Belize	Workstations in Antonio's Ristorante	Contests in Antonio's Ristorante	Field Trips at DEF CON 20
10:00 - 11:00	Hacking Roller Coasters and the Power Grid with Cell Phones Don Bailey	Code Breaking Museum NSA **10:00 - 17:00**	DoD Crime Scene Investigation **10:00 - 17:00**	Robots Katy Levinson
11:00 - 12:00	Hacking Venture Capital Phil Paul	DEFCON Kids TV Production DH & Goodson **11:00 - 17:00**	Hacker Board Games	Lockpicking and Hardware Hacking Villages
12:00 - 13:00	Go Eat!	Go Eat!	Go Eat!	Go Eat!
13:00 - 14:00	Building the DEFCON Kids App Thomas Leavy	3D Printing with My MakerBot Joe Grand **13:00 - 17:00**	3D Designs **13:00 - 17:00**	Contests Area and Vendor Area
14:00 - 15:00	Fight for Your Right... Marcia Hoffman Kurt Opsahl	Building the DEFCON Kids App Thomas Leavy **14:00 - 17:00**	The Shark Tank	Old School Hacking Kevin Poulsen
15:00 - 16:00	Cyber Patriot— A Student's Perspective Kevin Houk	EFF Workstation Marcia Hoffman	EFF Contest	Hacking the GoogleTV Amir Zenofex Etemadieh
16:00 - 17:00	Hacking as Practice for 21st Century Life: Preparing the World for a New Species Richard Thieme	Cryptoglass Clues Nic0	Cryptoglass Clues	How to Hack all the transport network of a country Alberto Garcia
17:00 - 18:00	Go Eat!	Go Eat!	Go Eat!	Go Eat!
18:00 - 19:00				Awards Ceremony
19:00 - 21:00				Awards Ceremony

PRESENTATIONS

Welcome / Making the DEF CON 20 Badge

THE DARK TANGENT
FOUNDER, DEF CON AND BLACK HAT
LOST
DT will address the con and officially open DEF CON 20. Following his address LostboY will enter into the story of mystery and imagination that is the badge game this year. (Oh, and talk about the making of the badge as well – as much as he can sans spoilers.) The dual-phase nature of the contest will also be discussed, which includes hardware hacks/modifications as well as solving the cryptographic puzzle challenges. Finally we'll talk about the joys and pains of this year's badge fabrication, which was all done in the USA.

Before, During, and After

WITH JASON SCOTT, GAIL THACKERAY AND DEAD ADDICT.

As you may have heard, in honor of our 20th anniversary, we have a DEF CON Documentary in the making by none other than Jason Scott of textfiles.com! At the beginning of this hour he will give you a quick sneak peek of the film and maybe discuss a few juicy tidbits!

Up next will be Gail Thackery and Dead Addict, to give a special introduction to this years VIP.

Twenty years ago, Dead Addict practically begged Gail Thackeray to appear at DEF CON, even though she was actively prosecuting several of his close friends. Since then the government (law enforcement, military, and intelligence community) has actively participated in DEF CON; to the point where we've been given the moniker 'FED CON'. Dead Addict will discuss the evolving relationship between government, the hacker community, and the civil liberties community. While obviously at odds with each other in some areas, there is also shared ground between these groups. This year he was happy to be able invite Gail again, this time not begging as much, and thankfully she isn't prosecuting any of his friends.

When Gail first spoke at DEF CON 1 there was no world wide web, state sponsored computer warfare was the stuff of science fiction, and international mafias had yet to become major players in computer crime.Internationally known for her role in Operation Sundevil, the former prosecuting attorney will discuss the changes in the computer security legal landscape since she first spoke at DEF CON. She will also discuss the evolution of the relationship between the computer security researcher community and law enforcement and government.

Gail Thackeray is a former Assistant Attorney General and Special Counsel recently retired from the Arizona Attorney General's Office. Her career prosecuting electronic crimes included the investigation and prosecution of early infrastructure attacks on a telephone network and a power company, as well as numerous fraud, cyberstalking and intrusion crimes. She participated in the nationwide Secret Service hacker investigation known as "Operation Sundevil" and attended the firstDEF CONConference. She currently works at the Arizona Counter Terrorism Information Center as a computer forensic examiner. She has a B.A. from Vassar College, a J.D. from Syracuse University, and earned the CFCE forensics certification from the International Association of Computer Investigative Specialists (IACIS).

Gail and Dead Addict will be introducing our special guest General Keith B. Alexander, Commander of U.S. Cyber Command and Director of the National Security Agency.

Shared Values, Shared Responsibility

GENERAL KEITH B. ALEXANDER
COMMANDER, U.S. CYBER COMMAND (USCYBERCOM) AND DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (NSA/CSS)
We as a global society are extremely vulnerable and at risk for a catastrophic cyber event. Global society needs the best and brightest to help secure our most valued resources in cyberspace: our intellectual property, our critical infrastructure and our privacy. DEF CON has an important place in computer security. It taps into a broad range of talent and provides an unprecedented diversity of experiences and expertise to solve tough problems. The hacker community and USG cyber community share some core values: we both see the Internet as an immensely positive force; we both believe information increases in value by sharing; we both respect protection of privacy and civil liberties; we both believe in the need for oversight that fosters innovation, doesn't pick winners and losers, and retains freedom and flexibility; we both oppose malicious and criminal behavior. We should build on this common ground because we have a shared responsibility to secure cyberspace.

General Keith B. Alexander is the Commander, U.S. Cyber Command (USCYBERCOM) and Director, National Security Agency/Chief, Central Security Service (NSA/CSS). As Commander, USCYBERCOM, he oversees planning, coordinating and conducting operations and defense of DoD computer networks. As Director, NSA/Chief, CSS, he oversees a DoD agency with national foreign intelligence, combat support, and U.S. national security information system protection responsibilities. GEN Alexander holds a B.S. from the U.S. Military Academy, a M.S. in Business Administration from Boston University, a M.S. in Systems Technology (Electronic Warfare) and a M.S. in Physics from the Naval Post Graduate School, and a M.S. in National Security Strategy from the National Defense University.

Def Con 101 [panel]

HIGHWIZ
MODERATOR
PYRO, ROAMER, LOCKHEED, ALXROGAN, LOST , FLIPPER
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.

Breaking Wireless Encryption Keys

DAKAHUNA

Cracking Wireless encryption keys is a fundamental capability that should be in every penetration tester's skill set. This talk will walk you through the basic steps necessary to break Wireless Encryption Protocol (WEP) and steps to perform dictionary and brute force attacks against Wi-Fi Protected Access (WPA & WPA2).

Intro to Digital Forensics: Tools & Tactics

RIPSHY, HACKAJAR

Putting up a flag and asking for help on the Internet is not for the faint of heart. When you simply want to get started with information security, hacking or just playing around with the vulnerabilities of computer systems, asking the right question to the right person is a crap shoot. Tired of being on the outside looking in? This 101 talk will help you get your feet wet! It will provide you the basic knowledge required when starting out in the InfoSec scene. Afraid to ask someone what the best NMap toggles are? Can't even get your metasploit running? Having trouble decoding your tcpdumps? We can help! Spend 50 min. with us and jump start the next 50 years of your life!

The Cerebral Source Code

SIVIAK

YOU: are part of the problem. You should count yourself among the ranks of the unprepared. You are under-educated and fooling yourself. You are sheep, you just don't know any better... but ignorance is no excuse. You know that much.

Navigating the world of Social Engineering is often portrayed with the image of "Jedi mind-tricks" and labeled with terms like "The Art of Deception"... These are all just ploys to convey mysticism, sell books and add value to a skill based on common sense, perception and the ability to think further than the end of your own nose.

It's time to remove the wool and learn what Social Engineering is and how it works. Welcome to a crash course in the oldest CLI.... Bring a helmet.

Screw the Planet, Hack the Job!

ROAMER, LOCKHEED, ALXROGAN

Have you ever wondered how you can translate your mad skillz into an actual job? Does coming to DEF CON even help you get there? Four members of the DEF CON staff will astound you with the stories of how they took their experiences at DEF CON and turned them into the jobs of their dreams. Despite using their DEF CON experiences to obtain these jobs, they represent four completely different industries: Government, Energy, Health Care, and the Video Game Industry in a variety of different job functions. Learn from their experience and find out what they look for (from the community?) when they need to fill positions in their respective industries.

Hf Skiddies Suck, Don't Be One. Learn Some Basic Python

TERRENCE 'TUNA' GARREAU

Fuck a bunch of skiddie tools acquired from bobo forums. One does not have to be a master to write their own shit. Yoda said it best get off your dick and write yourself some Python (Just don't show it to Highwiz he might bite it). Also always remember to stay in the the wizards good graces or you will find yourself publicly humiliated. You can come to this talk and find out how to be humiliated publicly but also: learn some python from a hackers perspective. Oh yea: Dongs, Schlongs, and Turds.

Hacking the Hackers: How Firm is Your Foundation?

LOST

Since this is DC101, I've got some things I want to get off my chest – a brief overview of 'foundational' hacker knowledge that I personally believe all hackers should have or would want – from subculture references to numerical oddities, this will be a meat space core dump of an ADD-OCD hacker. (ADD-OCD: I'm constantly changing what I'm completely obsessed about.) Topics will include mathematics, linguistics, programming, hardware, DEF CON, robotics, and more. A veritable cornucopia of fun. Or not.

Introduction to Lockpicking and Bypassing Physical Security

DR. TRAN

Everyone relies on their locks to keep things secure. From front doors to filing cabinets, they give us the sense of security that no one else can get inside without the proper key. However, in reality, most locks can be picked trivially without any evidence of exploitation. You will learn how and why lockpicking works as well as what manufacturers have done to protect against such shenanigans.

Owning Bad Guys [and Mafia] With Javascript Botnets

CHEMA ALONSO
SECURITY RESEARCHER, INFORMATICA64
MANU 'THE SUR'
PENETRATION TESTER, INFORMATICA64
Man in the middle attacks are still one of the most powerful techniques for owning machines. In this talk MITM schemas in anonymous services are going to be discussed. Then attendees will see how easily a botnet using javascript can be created to analyze that kind of connections and some of the actions people behind those services are doing... in real. It promises to be funny.

The Darknet of Things, Building Sensor Networks That Do Your Bidding

ANCH
OMEGA
The Internet of Things... It is coming, wearing hardware that communicates across the Internet is starting to become a reality, chips are getting smaller, as a society we are connected all the time... Building these devices is easier than we thought, putting them onto a network that is ours... EVEN BETTER! Come experience the Darknet of Things. Learn what we built, how we built it, and why. Learn how to get involved with a new community project, see what some of the DEF CON groups have been working on. Most importantly, learn how you can connect to the Darknet of Things.

Drones!

CHRIS ANDERSON
EDITOR-IN-CHIEF, WIRED MAGAZINE
Thanks to the plummeting cost of powerful motion sensors like those found in smartphones, the technology to create military-class autopilots is available to all. Over the past five years, the DIY Drones community has created a series of open source unmanned aerial vehicles (UAV), from fully-autonomous planes, helicopters, quadcopters, hexacopters, rovers and more, which cost just a few hundred dollars — less than 1% the cost of equivalent military drones. As a result there are now more than 10,000 of them in use — more than the US Military. As DIY drones go mainstream, what are the practical applications that will emerge, and the legal, ethical and economic implications? How does open source change the regulatory aspects of drones? And will the rise of "personal drones" have a similar social impact as "personal computers" did?

<6Hz or Bust: Def Con

ATLAS
DOOM CORPORATION
Wifi is cool and so is cellular, but the real fun stuff happens below the 6Hz line. Medical systems, mfg plant/industrial systems, cell phones, power systems, it's all in there!

atlas and some friends set out to turn pink girltech toys into power-systems-attack tools. Through several turns and changes, the cc1111usb project was born, specifically to make attacking these systems easier for all of you. With a $50 USB dongle, the world of ISM sub-GHz is literally at your fingertips.

PRESENTATIONS

New and improved! If you missed it at shmoocon, here's your chance to see the intro to this fun new world. If you caught it at shmoo, come to the talk and prove your <ghz prowess and wirelessly hack a special pink girl's toy target!

Blind XSS

ADAM 'EVILPACKET' BALDWIN
CHIEF SECURITY OFFICER, &YET

This talk will announce the release and demonstrate the xss.io toolkit. xss.io is a platform to help ease cross-site scripting (xss) exploitation and specifically for this talk identification of blind xss vectors. Think drag and drop exploits post xss vuln identification. For blind xss, xss.io is a callback and hook manager for intel collected by executed and non-executed but accessed payloads.

Should the Wall of Sheep Be Illegal? A Debate Over Whether and How Open WiFi Sniffing Should Be Regulated

KEVIN BANKSTON
SENIOR COUNSEL & DIRECTOR OF FREE EXPRESSION, CENTER FOR DEMOCRACY AND TECHNOLOGY
MATT BLAZE
DIRECTOR, DISTRIBUTED SYSTEMS LAB, UNIVERSITY OF PENNSYLVANIA
JENNIFER GRANICK
GENERAL COUNSEL, WORLDSTAR, LLC

Prompted by the Google Street View WiFi sniffing scandal, the question of whether and how the law regulates interception of unencrypted wireless communications has become a hot topic in the courts, in the halls of the FCC, on Capitol Hill, and in the security community. Are open WiFi communications protected by federal wiretap law, unprotected, or some strange mix of the two? (Surprise: it may be the last one, so you'll want to come learn the line between what's probably illegal sniffing and what's probably not.)

More importantly, what *should* the law be? Should the privacy of those who use WiFi without encryption be protected by law, or would regulating open WiFi sniffing pose too great a danger to security research and wireless innovation, not to mention DEF CON traditions like the Wall of Sheep? Join legal expert Kevin Bankston and technical expert Matt Blaze as they square off in a debate to answer these questions, moderated by Jennifer Granick. (Surprise: the lawyer is the one arguing for regulation.)

Cryptohaze Cloud Cracking

BITWEASIL
LEAD DEVELOPER, CRYPTOHAZE TOOLS

Bitweasil goes through the latest developments in the Cryptohaze GPU based password cracking suite. WebTables is a new rainbow table technology that eliminates the need to download rainbow tables before using them, and the new Cryptohaze Multiforcer is an open source, GPLv2, network enabled platform for password cracking that is easy to extend with new algorithms for specific targets. The Cryptohaze Multiforcer supports CUDA, OpenCL, and CPU code (SSE, AVX, etc). All of this is aimed at either the pentester who can't spray hashes to the internet, or the hacker who would rather not broadcast what she obtained to pastebin scrapers.

Overwriting the Exception Handling Cache Pointer Dwarf Oriented Programming

RODRIGO RUBIRA BRANCO
VULNERABILITY & MALWARE RESEARCH LABS, QUALYS
JAMES OAKLEY
PROGRAMMER
SERGEY BRATUS
RESEARCH ASS'T PROFESSOR, COMP. SCIENCE, DARTMOUTH COLLEGE

This presentation describes a new technique for abusing the DWARF exception handling architecture used by the GCC tool chain. This technique can be used to exploit vulnerabilities in programs compiled with or linked to exception-enabled parts. Exception handling information is stored in bytecode format, executed by a virtual machine during the course of exception unwinding and handling. We show how a malicious attacker could gain control of those structures and inject bytecode for malicious purposes. This virtual machine is actually Turing-complete, which means that it can be made to run arbitrary attacker logic.

Exploit Archaeology: Raiders of the Lost Payphones

JOSH BRASHARS
PENETRATION TESTER, MEMBER DC 949

Payphones. Remember those? They used to be a cornerstone of modern civilation, available at every street corner, gas station, or any general place of commerce. For decades, hackers and phone phreaks crowded around them as an altar to high technology and a means to "reach out and touch someone".

Fast forward to today, most people have mobile phones. Payphones installed decades earlier are now more of a memorial to a time long gone by. Covered with grime and graffitti, forgotten, relegated to the realm of drug dealers and other undesirables. But they're still around, and they're more vulnerable than ever.

This talk will review modern hacking techniques applied to retro hardware. We'll cover owning payphones and how they can be retrofitted with new technologies to turn them into the ultimate low profile hacking platform to compromise your organizations network. There will be demos of payphone hacking on stage, as well as using the payphone to intercept voice phone traffic. We'll also reveal a new tool to automate the exploitation of payphones and relate how (like with all forms of archaelogoy) learning about old platforms can help us secure modern architecture.

Hardware Backdooring is Practical

JONATHAN BROSSARD
TOUCAN SYSTEM

This presentation will demonstrate that permanent backdooring of hardware is practical. We have built a generic proof of concept malware for the intel architecture, Rakshasa, capable of infecting more than a hundred of different motherboards. The first net effect of Rakshasa is to disable NX permanently and remove SMM related fixes from the BIOS, resulting in permanent lowering of the security of the backdoored computer, even after complete earasing of hard disks and reinstallation of a new operating system. We shall also demonstrate that preexisting work on MBR subvertions such as bootkiting and preboot authentication software bruteforce can be embedded in Rakshasa with little effort. Moreover, Rakshasa is built on top of free software, including the Coreboot project, meaning that most of its source code is already public. This presentation will take a deep dive into Coreboot and hardware components such as the BIOS, CMOS and PIC embedded on the motherboard, before detailing the inner workings of Rakshasa and demo its capabilities. It is hoped to raise awareness of the security community regarding the dangers associated with non open source firmwares shipped with any computer and question their integrity. This shall also result in upgrading the best practices for forensics and post intrusion analysis by including the afore mentioned firmwares as part of their scope of work.

DIY Electric Car

DAVE BROWN

Electric Vehicles are an exciting area of developing technology entering the mainstream market. Every major manufacturer is working on new hybrid and electric vehicles but prices will be high and options few for years to come.

As with many industries, a DIY approach can yield similar results for much less cost, while creating something truly unique.

This talk will explore the possibilities and procedures involved in creating your own electric vehicle. Topics addressed will include the whys and hows, with an emphasis on the options available to tailor your conversion to match your time, budget, and performance needs.

Tenacious Diggity: Skinny Dippin' in a Sea of Bing

FRANCIS BROWN
MANAGING PARTNER – STACH & LIU, LLC
ROB RAGAN
SENIOR SECURITY ASSOCIATE – STACH & LIU, LLC

All brand new tool additions to the Google Hacking Diggity Project – The Next Generation Search Engine Hacking Arsenal. As always, all tools are free for download and use.

When last we saw our heroes, the Diggity Duo had demonstrated how search engine hacking could be used to take over someone's Amazon cloud in less than 30 seconds, build out an attack profile of the Chinese government's external networks, and even download all of an organization's Internet facing documents and mine them for passwords and secrets. Google and Bing were forced to hug it out, as their services were seamlessly combined to identify which of the most popular websites on the Internet were unwittingly being used as malware distribution platforms against their own end-users.

Now, we've traveled through space and time, my friend, to rock this house again...

True to form, the legendary duo have toiled night and day in the studio (a one room apartment with no air conditioning) to bring you an entirely new search engine hacking tool arsenal that's packed with so much tiger blood and awesome-sauce, that it's banned on 6 continents. Many of these new Diggity tools are also fueled by the power of the cloud and provide you with vulnerability data faster and easier than ever thanks to the convenience of mobile applications.

KinectasploitV2: Kinect Meets 20 Security Tools

JEFF BRYNER
POWNLABS, OWNER

Last year saw the release of Kinectasploit v1 linking the Kinect with Metasploit in a 3D, first person shooter environment. What if we expanded Kinectasploit to use 20 security tools in honor of DEF CON's 20th anniversary?!

Fuzzing Online Games

ELIE BURSZTEIN
RESEARCHER, GOOGLE
PATRICK SAMY
RESEARCH ENGINEER,, STANFORD UNIVERSITY

Fuzzing online games to find interesting bugs requires a unique set of novel techniques.

In a nutshell the lack of direct access to the game server and having to deal with clients that are far too complex to be easily emulated force us to rely on injecting fuzzing data into a legitimate connections rather than use the standard replay execution approach. Top that with heavily encrypted and complex network protocols and you start to see why we had to become creative to succeed :)

In this talk, we will discuss and illustrate the novels techniques we had to develop to be able to fuzz online games, including how to successfully inject data into a gaming sessions and how to instrument the game memory to know that our fuzzing was successful. We will also tell you how to find and reverse the interesting part of the protocol, and how to decide when to perform the injection.

The Open Cyber Challenge Platform

LINDA C. BUTLER

Everyone from MIT to the DoD have agreed that teaching cyber security using cyber challenges, where groups of students attack or defend a live network, has proven to be an incredibly effective educational tactic. Unfortunately, current cyber challenge tools also suffer from being very hard to configure, and/or very expensive, and/or limited to certain audiences (e.g. the military), which makes them inaccessible to high schools, colleges, and smaller organizations. The Open Cyber Challenge Platform aims to help fix this by providing a free, open-source, cyber challenge software platform that is reasonable in terms of cost of required hardware and required technical installation/maintenance expertise, as well as easily extensible to allow the vast open source community to provide additional modules that reflect new challenges and scenarios. If you're interested in the future of cyber-security education, or simply just want to learn about a new potential training tool, come check out the OCCP.

Into the Droid: Gaining Access to Android User Data

THOMAS CANNON
DIRECTOR OF R&D, VIAFORENSICS

This talk details a selection of techniques for getting the data out of an Android device in order to perform forensic analysis. It covers cracking lockscreen passwords, creating custom forensic ramdisks, bypassing bootloader protections and stealth real-time data acquisition. We'll even cover some crazy techniques – they may get you that crucial data when nothing else will work, or they may destroy the evidence!

Forensic practitioners are well acquainted with push-button forensics software. They are an essential tool to keep on top of high case loads – plug in the device and it pulls out the data. Gaining access to that data is a constant challenge against sophisticated protection being built into modern smartphones. Combined with the diversity of firmware and hardware on the Android platform it is not uncommon to require some manual methods and advanced tools to get the data you need.

This talk will reveal some of the techniques forensic software uses behind the scenes, and will give some insight into what methods and processes blackhats and law enforcement have at their disposal to get at your data. Free and Open Source tools will be released along with this talk to help you experiment with the techniques discussed.

Panel: Meet the Feds 1

JIM CHRISTY
MODERATOR
JON IADONISI
WHITE CANVAS GROUP
LEON CAROLL
TECHNICAL ADVISOR, CBS'S NCIS, EX-NCIS
RICH MARSHALL
FOUNDER AND PRESIDENT, X-SES CONSULTANTS, LLC
ANDY FRIED
EX-IRS
DAVID MCCALLUM
CBS'S NCIS
JUSTIN WYKES
NW3C

Did you ever wonder if the Feds were telling you're the truth when you asked a question? Join current and former federal agents from numerous agencies to discuss cyber investigations and answer your burning questions. Enjoy the opportunity to grill 'em and get down to the bottom of things!

Agencies that will have representatives include: Defense Cyber Crime Center (DC3), National White Collar Crime Center (NWC3), US Department of Treasury, Internal R evenue Service (IRS), and the US Navy SEALs. This year,

PRESENTATIONS

the "Meet the Feds" panel has gone Hollywood with special guests – Mr. David McCallum and Mr. Leon Carroll from CBS's NCIS!

Panel: Meet the Feds 2: Policy

JIM CHRISTY
MODERATOR
JERRY DIXON
EX-DHS
MARK WEATHERFORD
DHS
DR. LINTON WELLS
NDU
ROD BECKSTROM
EX-DHS
MISHEL KWON
EX-USCERT
RILEY REPKO
EX-GSD
BOB LENTZ
EX-OSD/NII

Did you ever wonder if the Feds were telling you're the truth when you asked a question? Join current and former federal agents from numerous agencies to discuss cyber investigations and answer your burning questions. Enjoy the opportunity to grill 'em and get down to the bottom of things!

SIGINT and Traffic Analysis for the Rest of Us

SANDY CLARK
UNIVERSITY OF PENNSYLVANIA
MATT BLAZE
PROFESSOR AND LAB DIRECTOR, UNIVERSITY OF PENNSYLVANIA

Last year, we discovered practical protocol weaknesses in P25, a "secure" two-way radio system used by, among others, the federal government to manage surveillance and other sensitive law enforcement and intelligence operations. Although some of the problems are quite serious (efficient jamming, cryptographic failures, vulnerability to active tracking of idle radios, etc), many of these vulnerabilities require an active attacker who is able and willing to risk transmitting. So we also examined passive attacks, where all the attacker needs to do is listen, exploiting usability and key management errors when they occur. And we built a multi-city networked P25 interception infrastructure to see how badly the P25 security protocols do in practice (spoiler: badly).

This talk will describe the P25 protocols and how they failed, but will focus on the architecture and implementation of our interception network. We used off-the-shelf receivers with some custom software deployed around various US cities, capturing virtually every sensitive, but unintentionally clear transmission (and associated metadata) sent by federal agents in those cities. And by systematically analyzing the captured data, we often found that the whole was much more revealing than the sum of the parts. Come learn how to set up your own listening-post.

Bad (and Sometimes Good) Tech Policy: It's Not Just a DC Thing

CHRIS CONLEY
TECHNOLOGY & CIVIL LIBERTIES POLICY ATTORNEY, ACLU OF NORTHERN CALIFORNIA

Efforts at the federal level to pass laws like SOPA and CISPA and require that tech companies build backdoors into their services for law enforcement use have attacted widespread attention and criticism, and rightly so. But DC is far from the only place that officials are making decisions that impact the privacy and free speech rights of tech users. State and local officials are jumping into the fray as well, passing laws or creating policies that have immediate impact without the spotlight that accompanies federal action.

In this talk, I will survey several areas where state and local officials have recently been active, including warrantless location tracking, searches of student and employee devices and online accounts, automated license plate recognition, and DNA collection. I will highlight some of the best and worst policies coming from state and local officials. Most of all, I hope to convince you that keeping an eye on — and even taking time to educate — your local sheriff or state legislature may be just as important as protecting your freedoms at the national level.

Life Inside a Skinner Box: Confronting Our Future of Automated Law Enforcement

GREG CONTI
DIRECTOR, CYBER RESEARCH CENTER, WEST POINT
LISA SHAY
ASS'T PROFESSOR, ELECTRICAL ENGINEERING & COMPUTER SCIENCE, WEST POINT
GREG CONTI
ASS'T PROFESSOR, CUMBERLAND SCHOOL OF LAW, SAMFORD UNIVERSITY

From smart pajamas that monitor our sleep patterns to mandatory black boxes in cars to smart trash carts that divulge recycling violations in Cleveland, virtually every aspect of our lives is becoming instrumented and increasingly connected to law enforcement, government, and private entities. At the same time, these entities are incentivized to further collect, process, and punish in the name of financial advantage, public safety, or security. The trend of automated law enforcement is inescapable and touches every citizen. This talk will explore the implications of automated law enforcement, study the incentives at play, survey recent advances in sensing and surveillance technology, and will seek to answer the following questions and more. Were laws written with the idea of universal and perfect enforcement in mind?

Owning the Network: Adventures in Router Rootkits

MICHAEL COPPOLA
SECURITY CONSULTANT, VIRTUAL SECURITY RESEARCH

Routers are the blippy switchy boxes that make up the infrastructure of networks themselves, yet few administrators actually care to change the default login on these devices. Interestingly, nearly all consumer (SOHO) routers allow a user to reflash the device by uploading a (presumably vendor-provided) firmware image. By abusing this feature, it is possible for an attacker to craft his or her own malicious firmware image and execute arbitrary code on the device, granting full control over the OS, the network it manages, and all traffic passing through it. Additionally, interesting persistence and pivot opportunities are realized, allowing an attacker to maintain access or target internal hosts in a covert way.

Based on personal experience, we'll examine the process of backdooring firmware images for SOHO routers from start to finish. A generalized technique to backdoor firmware images will be outlined, and a new framework to abstract and expedite the process will be publicly released. Working examples will be presented which demonstrate the ability to pop shells, hide connections, sniff traffic, and create a router botnet of doom.

World War 3.0: Chaos, Control & the Battle for the Net

JOSHUA CORMAN
DIRECTOR OF SECURITY INTELLIGENCE, AKAMAI TECHNOLOGIES
DAN KAMINSKY
JEFF MOSS
FOUNDER, DEF CON AND BLACK HAT
ROD BECKSTROM
MICHAEL JOSEPH GROSS
CONTRIBUTING EDITOR, VANITY FAIR, MODERATOR

There is a battle under way for control of the Internet. Some see it as a fight between forces of Order (who want to superimpose existing, pre-digital power structures and their notions of privacy, intellectual property, security, and sovereignty onto the Net) and forces of Disorder (who want to abandon those old structures and let the will of the crowd control a new global culture). Yet this binary view of the conflict excludes the characters with the best chance of resolving it: those who know that control is impossible and chaos is untenable, a group that Vanity Fair, in an article called "World War 3.0," called "the forces of Organized Chaos." This panel gathers leading proponents of that worldview to discuss urgent issues of Internet governance, which may come to a head later this year in a Dubai meeting of the U.N.'s International Telecommunications Union. If government control and anarchistic chaos online are unacceptable, what exactly do the forces of organized chaos propose as an alternative? And what is the DEF CON community's role in helping to realize that vision of the Net?

Embedded Device Firmware Vulnerability Hunting Using FRAK, the Firmware Reverse Analysis Konsole

ANG CUI
RED BALLOON SECURITY

We present FRAK, the firmware reverse analysis konsole. FRAK is a framework for unpacking, analyzing, modifying and repacking the firmware images of proprietary embedded devices. The FRAK framework provides a programmatic environment for the analysis of arbitrary embedded device firmware as well as an interactive environment for the disassembly, manipulation and re-assembly of such binary images.

We demonstrate the automated analysis of Cisco IOS, Cisco IP phone and HP LaserJet printer firmware images. We show how FRAK can integrate with existing vulnerability analysis tools to automate bug hunting for embedded devices. We also demonstrate how FRAK can be used to inject experimental host-based defenses into proprietary devices like Cisco routers and HP printers.

Looking Into The Eye Of The Meter

CUTAWAY
INGUARDIANS, INC.

When you look at a Smart Meter, it practically winks at you. Their Optical Port calls to you. It calls to criminals as well. But how do criminals interact with it? We will show you how they look into the eye of the meter. More specifically, this presentation will show how criminals gather information from meters to do their dirty work. From quick memory acquisition techniques to more complex hardware bus sniffing, the techniques outlined in this presentation will show how authentication credentials are acquired. Finally, a method for interacting with a meter's IR port will be introduced to show that vendor specific software is not necessary to poke a meter in the eye.

This IS the talk that was not presented at ShmooCon 2012 in response to requests from a Smart Grid vendor and the concerns of several utilities. We have worked with them. They should be okay with this.....should.....

SQL Injection to MIPS Overflows: Rooting SOHO Routers

ZACHARY CUTLIP
SECURITY RESEARCHER, TACTICAL NETWORK SOLUTIONS

Three easy steps to world domination:

Pwn a bunch of SOHO routers.
???
Profit

I can help you with Step 1. In this talk, I'll describe several 0-day vulnerabilities in Netgear wireless routers. I'll show you how to exploit an unexposed buffer overflow using nothing but a SQL injection and your bare hands. Additionally, I'll show how to use the same SQL injection to extract arbitrary files from the file systems of the wifi routers. This presentation guides the audience through the vulnerability discovery and exploitation process, concluding with a live demonstration. In the course of describing several vulnerabilities, I present effective investigation and exploitation techniques of interest to anyone analyzing SOHO routers and other embedded devices.

DC Recognize Awards

JEFF MOSS
FOUNDER, DEF CON AND BLACK HAT
JERICHO
RUSS ROGERS
CONTEST GURU

DEF CON is proud to announce the 2nd annual DEF CON awards ceremony, renamed the DC Recognize Awards. These awards are given to deserving individuals in the community, industry, and media.

You voted, so come see who made the cut.

Hacking Humanity: Human Augmentation and You

CHRISTIAN 'QUADDI' DAMEFF
THIRD YEAR MEDICAL STUDENT
JEFF 'R3PLICANT' TULLY
THIRD YEAR MEDICAL STUDENT

You've played Deus Ex. You've seen Robocop. You've read Neuromancer. You've maybe even wondered just what dark mix of technology and black magic keeps the withered heart of Richard "Dick" Cheney pumping coronary after coronary. Now it's time to get off the couch and put down the controller. Human augmentation is no longer constrained to the world of speculative fiction and vice-presidential medicine; biomechanical interfaces are an exploding area of active research, development, and implementation. And they're here to stay.

Join medical student/hacker enthusiasts quaddi and r3plicant for a fun-filled tour through the brave new world of the latest and greatest in this exciting new melding of medicine and technology. From the simplest insulin pump to the latest gyroscopic prosthesis for wounded veterans, from the full body DARPA developed exoskeleton of the future to the changes currently being implemented in our most fundamental building blocks, this talk explores what was, what is and what will be in the future of human augmentation, and more importantly, what you need to know to get started down the path to Robocop glory.

Connected Chaos: Evolving the DCG/Hackspace Communication Landscape

BLAKDAYZ
MODERATOR
ANARCHY ANGEL, ANCH, DAVE MARCUS, NICK FARR

As hackers, we have access to tremendous informational power. At our individual hackerspaces and DCGs we build communities of like minded hackers that push the limits of technology. But have we gone far enough in building a global hacking community that celebrates diversity and unleashes world-changing genius?

We can accelerate the opportunity for community and change through technology. Take a seat and hear what resources are available to the groups and hackspaces in your area. By connecting our chaos, we can transcend the isolation and polarization that dominates much of our communities. We can unite and empower. Join the discussion and chaos so we can evolve the way our community will be connected.

How do you change the world? One connected hacker, hackerspace and DCG at a time.

Not-So-Limited Warranty: Target Attacks on Warranties for Fun and Profit

DARKRED

Frequently people consider a serial number as nothing but a number but in this presentation you will be shown the multitude of ways in which an attacker could utilize serial numbers to hurt

MAP

RIO ALL-SUITE HOTEL & CASINO

PRESENTATIONS

you,to hurt companies as well as to track your movements. A brief primer on the function and use of serial numbers in the real world will be provided. Focusing on Apple, Amazon and Pringles and providing in-depth insight into the varying degrees of trust a serial number will gain you. Attack vectors ranging from Apple to Pringles and everywhere in between along with points about how to prevent similar tragedies from occurring with your product.

DivaShark - Monitor your flow

ROBERT DEATON

Analyzing live network traffic is nothing new but the tools still seem limited. Wireshark is great for post capture analysis but when the packets are coming at you live, nothing currently gives your stream or session level visibility. How many times have you clicked 'Follow this stream' just to have that stream update and you have to reprocess the entire PCAP? That's great when it's just your machine but when you're monitoring a network, it limits your view and is a pain. As more traffic adds, this problem grows and makes life for your little netbook quite painful. Enter DivaShark – your live packet capture solution.

Beyond the War on General Purpose Computing: What's Inside the Box?

CORY DOCTOROW
AUTHOR, ACTIVIST, BLOGGER, CO-EDITOR OF BOINGBOING.NET

Assuming the failure of all the calls to regulate PCs and the Internet because people might do bad things with them, what then? Civil war, that's what. The su/user split we inherited from multiuser systems has given us a false intuition: that owners of computers, and not their users, should set policy on them. How will that play out when your car, house, legs, ears and heart are driven by computers that you don't own?

Sploitego - Maltego's (local) Partner in Crime

NADEEM DOUBA
CYGNOS IT SECURITY

Have you ever wished for the power of Maltego when performing internal assessments? Ever hoped to map the internal network within seconds? Or that Maltego had a tad more aggression? Sploitego is the answer. In the presentation we'll show how we've carefully crafted several local transforms that gives Maltego the ooomph to operate nicely within internal networks. Can you say Metasploit integration? ARP spoofing? Passive fingerprinting? SNMP hunting? This all is Sploitego. But wait – there's more. Along the way we'll show you how to use our awesome Python framework that makes writing local transforms as easy as 'Hello World'.

Not So Super Notes: How Well Does US Dollar Note Security Prevent Counterfeiting?

MATTHEW DUGGAN
MEMBER OF TECHNICAL STAFF, VMWARE INC

The security of US dollar notes is paramount for maintaining their value and safeguarding the US and dependent economies. Counterfeiting has historically been a crime of high sophistication, but has the prevalence of affordable color scanning and printing equipment changed that? This talk analyzes the security features of US dollars to determine the minimum sized organization that could successfully execute an attack.

Post Metasploitation: Improving Accuracy and Efficiency in Post Exploitation Using the Metasploit Framework

EGYPT
DEVELOPER, RAPID7

As many in this community have echoed, shell is just the beginning. Owning a box is all well and good, but where do you go from there? Everyone has their own secret sauce for furthering their access after gaining a foothold. This talk will focus on the techniques, from simple to advanced, available for post exploitation using the Metasploit Framework.

The Paparazzi Platform: Flexible, Open-Source, UAS Software and Hardware

ESDEN, DOTAERO, MISTERJ, CIFO

This presentation introduces the Paparazzi framework, an Open-Source (GPL3 and OSHW CC-by-SA) software and hardware robotics platform focused on Unmanned Aerial Systems (UASes). Paparazzi's power and flexibility enable rapid development and robust control of diverse vehicle types – from fixed-wing airplanes to multicopters and transitioning aircraft – while its open nature permit customization and integration with other systems.

We show the capabilities of the platform and some achievements from all around the world with this platform. We also will show what we are working on and introduce it to the public.

What will you do with that powerful tool?

The Paparazzi autopilots, a multicopter, and the Quadshot – a VTOL, multirotor, transitioning flying wing – are presented.

Hacking the Google TV

AMIR 'ZENOFEX' ETEMADIEH
CJ HERES
DAN ROSENBERG
TOM 'TDWENG' DWENGER

This presentation will focus on the current GoogleTV devices, including X86 platform details, and the exhaustive security measures used by each device. The presentation will also include video demonstrations of previously found bugs and exploits for each GoogleTV device and includes specific details about how each bug works. Furthermore, we will include interesting experiences that the team has encountered along the way. Finally the talk will be capped off with the release of multiple unpublished GoogleTV exploits which will allow unsigned kernels across all x86 devices (Revue / Sony GoogleTV).

Owned in 60 Seconds: From Network Guest to Windows Domain Admin

ZACK FASEL

Their systems were fully patched, their security team watching, and the amateur pentesters just delivered their "compliant" report. They thought their Windows domain was secure. They thought wrong.

Zack Fasel (played by none other than Angelina Jolie) brings a New Tool along with New methods to obtain Windows Integrated Authentication network requests and perform NTLM relaying both internally and externally. The Goal? Start off as a nobody and get domain admin (or sensitive data/access) in 60 seconds or less on a fully patched and typically secured windows environment. The Grand Finale? Zack demonstrates the ability to *externally* gain access to a Windows domain user's exchange account simply by sending them an email along with tips on how to prevent yourself from these attacks.

In just one click of a link, one view of an email, or one wrong web request, this new toolset steals the identity of targeted users and leverages their access. Call your domain admins, hide your road warriors, and warn your internal users. Zack will change the way you think about Windows Active Directory Security and trust relationships driving you to further harden your systems and help you sleep at night.

Owned in 60 Seconds. Coming This Summer.

Hellaphone: Replacing the Java in Android

JOHN FLOREN
SENIOR MEMBER OF TECHNICAL STAFF, SANDIA NATIONAL LABS

Android is the only widespread open-source phone environment available today, but actually hacking on it can be an exercise in frustration, with over 14 million lines of code (not counting the Linux kernel!), build times in the hours, and the choice of writing Java or C++/JNI. Add in security debacles like the CarrierIQ affair or the alleged man-in-the-middle attacks at the last DEF CON and Android starts to seem less attractive.

We wanted a phone that's easy to hack on, with a quick development turnaround time. By killing off the Java layer of Android and only loading the underlying Linux system, we found a useful, relatively light-weight platform for further development. We then adapted the Inferno operating system to run on our phones, eventually getting a graphical phone environment in under 1 million lines of code, including a phone application, an SMS app, several text editors, a shell, a compiler, a web browser, a mail client, and even some games. The actual core of the Inferno OS is small and simple enough for one person to read, understand, audit, and hack on; applications are similarly simple and easy to write.

This talk discusses in greater depth our motivations and the methods we used to adapt Android phones to new and excitingly broken purposes. If the Demo Gods are kind, there will also be a demonstration of the Inferno phone environment.

Hacking [redacted] Routers

FX
LEADER, PHENOELIT GROUP, RECURITY LABS
GREG
RECURITY LABS

[Redacted] routers are no longer devices only seen in [Redacted]. Entire countries run their Internet infrastructure exclusively on these products and established tier 1 ISPs make increasing use of them. However, very little is known of [Redacted]'s Software Platform and its security. This presentation will introduce the architecture, special properties of configurations and services as well as how to reverse engineer the OS. Obviously, this is done only to ensure compatibility with router products of other vendors ;) Routers might be still hurt in the process.

Demorpheus: Getting Rid of Polymorphic Shellcodes in Your Network

SVETLANA GAIVORONSKI
PHD STUDENT, MOSCOW STATE UNIVERSITY
DENNIS GAMAYUNOV
SENIOR RESEARCHER, MOSCOW STATE UNIVERSITY

One of the most effective techniques used in CTF is the usage of various exploits, written with the help of well-known tools or even manually during the game. Experience in CTF participation shows that the mechanism for detecting such exploits is able to significantly increase the defense level of the team.

In this presentation we propose an approach and hybrid shellcode detection method, aimed at early detection and filtering of unknown 0-day exploits at the network level. The proposed approach allows us to summarize capabilities of shellcode detection algorithms developed over recent ten years into optimal classifiers. The proposed approach allows us to reduce the total fp rate almost to 0, provides full coverage of shellcode classes detected by individual classifiers and significantly increases total throughput of detectors. Evaluation with shellcode datasets, including Metasploit Framework 4.3 plain-text, encrypted and obfuscated shellcodes, benign Win32 and Linux ELF executables, random data and multimedia shows that hybrid data-flow classifier significantly boosts analysis throughput for benign data – up to 45 times faster than linear combination of classifiers, and almost 1.5 times faster for shellcode only datasets.

New Techniques in SQLi Obfuscation: SQL never before used in SQLi

NICK GALBREATH

SQLi remains a popular sport in the security arms-race. However, after analysis of hundreds of thousands of real world SQLi attacks, output from SQLi scanners, published reports, analysis of WAF source code, and database vendor documentation, both SQLi attackers and defenders have missed a few opportunities. This talk will iterate through the dark corners of SQL for use in new obfuscated attacks, and show why they are problematic for regular-expression based WAFs. This will point the way for new directions in SQLi research for both offense and defense.

Uncovering SAP Vulnerabilities: Reversing and Breaking the Diag Protocol

MARTIN GALLO
SECURITY CONSULTANT, CORE SECURITY

This talk is about taking SAP penetration testing out of the shadows and shedding some light into SAP Diag, by introducing a novel way to uncover vulnerabilities in SAP software through a set of tools that allows analysis and manipulation of the SAP Diag protocol. In addition, we will show how these tools and the knowledge acquired while researching the protocol can be used for vulnerability research, fuzzing and practical exploitation of novel attack vectors involving both SAP's client and server applications: man-in-the-middle attacks, RFC calls injection, rogue SAP servers deployment, SAP GUI client-side attacks and more. As a final note, this presentation will also show how to harden your SAP installations and mitigate these threats.

Post-Exploitation Nirvana: Launching OpenDLP Agents over Meterpreter Sessions

ANDREW GAVIN
SECURITY CONSULTANT, VERIZON BUSINESS
MICHAEL BAUCOM
VICE PRESIDENT OF R&D, N2 NET SECURITY INC.
CHARLES SMITH
SOFTWARE DEVELOPER, N2 NET SECURITY INC.

OpenDLP is a free and open source agent-based data discovery tool that works against Microsoft Windows systems using appropriate authentication credentials. However, one drawback to OpenDLP is that its policy-driven approach makes it arduous to scan disjointed systems that are not part of a Windows domain or do not share the same authentication credentials. To fix this, OpenDLP can now launch its agents over Meterpreter sessions using Metasploit RPC without requiring domain credentials.

The Art of Cyberwar

KENNETH GEERS
NCIS CYBER SUBJECT MATTER EXPERT

The establishment of US Cyber Command in 2010 confirmed that cyberspace is a new domain of warfare. Computers are now both a weapon and a target. Future wars may even be fought over the ownership of IT infrastructure. Therefore, national security thinkers must find a way to incorporate cyber attack and defense into military doctrine as soon as possible. The world's most influential military treatise is Sun Tzu's Art of

PRESENTATIONS

War. Its wisdom has survived myriad revolutions in technology and human conflict, and future cyber commanders will find Sun Tzu's guidance beneficial. However, this presentation will also consider 10 revolutionary aspects of cyber war that will be difficult to fit into military doctrine.

SCADA Strangelove or: How I Learned to Start Worrying and Love the Nuclear Plants

SERGEY GORDEYCHIK
CHIEF TECHNICAL OFFICER, POSITIVE TECHNOLOGIES
DENIS BARANOV
PRINCIPAL RESEARCHER, POSITIVE TECHNOLOGIES
SERGEY GORDEYCHIK
PRINCIPAL RESEARCHER, POSITIVE TECHNOLOGIES

Modern civilization unconditionally depends on information systems. It is paradoxical but true that SCADA systems are the most insecure systems in the world. From network to application, SCADA is full of configuration issues and vulnerabilities. During our report, we will demonstrate how to obtain full access to a plant via:

– a sniffer and a packet generator
– FTP and Telnet
– Metasploit and oslq
– a webserver and a browser

About 20 new vulnerabilities in common SCADA systems including Simatic WinCC will be revealed in the report

Releases:
– modbuspatrol (mbpatrol) – free tool to discover and fingerprint PLC
– Simatic WinCC security checklist
– close to real-life exploit scenario for a Simatic WinCC based plant.

More Projects of Prototype This

JOE GRAND
ELECTRICAL ENGINEER, GRAND IDEA STUDIO
ZOZ
ROBOTICS ENGINEER

For 18 months, Joe Grand and Zoz Brooks were co-hosts of Discovery Channel's Prototype This, an engineering entertainment program that followed the real-life design process of a unique prototype every episode.

At DEF CON 17, Joe and Zoz talked about the show and a few of their favorite builds. The dynamic nerd duo returns to DEF CON 20 with design details and never-before-seen pictures and videos of even more ridiculous and crazy projects, including the Mind Controlled Car, Boxing Robots, Six-Legged All Terrain Vehicle, Get Up and Go, and Automated Pizza Delivery, each of which had to be designed and built in a matter of weeks.

Hacking Measured Boot and UEFI

DAN GRIFFIN
PRESIDENT, JW SECURE, INC.

There's been a lot buzz about UEFI Secure Booting, and the ability of hardware and software manufacturers to lock out third-party loaders (and rootkits). Even the NSA has been advocating the adoption of measured boot and hardware-based integrity checks. But what does this trend mean to the open source and hacker communities? In this talk I'll demonstrate measured boot in action. I'll also be releasing my new Measured Boot Tool which allows you to view Trusted Platform Module (TPM) boot data and identify risks such as unsigned early-boot drivers. And, I'll demonstrate how measured boot is used for remote device authentication.

Finally, I'll discuss weaknesses in the system (hint: bootstrapping trust is still hard), what this technology means to the consumerization trend in IT, and what software and services gaps exist in this space for aspiring entrepreneurs.

Exchanging Demands

PETER HANNAY
SECURITY RESEARCHER, PHD STUDENT

Smart phones and other portable devices are increasingly used with Microsoft Exchange to allow people to check their corporate emails or sync their calendars remotely. Exchange has an interesting relationship with its mobile clients. It demands a certain level of control over the devices, enforcing policy such as password complexity, screen timeouts, remote lock out and remote wipe functionality. This behavior is usually accepted by the user via a prompt when they first connect to Exchange. However, the protocol for updating these policies provides very little in the way of security and is quickly accepted by the device, often with no user interaction required.

In this talk we will focus on the remote wipe functionality and how a potential attacker could abuse this functionality to remotely wipe devices that are connected to Exchange. By impersonating an Exchange server and sending appropriate policy updates through a simple script we are able to erase all data on devices remotely without any need for authentication. The presentation will explain how this can be accomplished and show proof of concept code for Android & iOS devices.

Changing the Security Paradigm: Taking Back Your Network and Bringing Pain to the Adversary

SHAWN HENRY
CROWDSTRIKE

The threat to our networks is increasing at an unprecedented rate. The hostile environment we operate in has rendered traditional security strategies obsolete. Adversary advances require changes in the way we operate, and "offense" changes the game.

Busting the BARR: Tracking 'Untrackable' Private Aircraft for Fun & Profit

DUSTIN HOFFMAN
PRESIDENT & SENIOR ENGINEER, EXIGENT SYSTEMS INC.
SEMON REZCHIKOV
INDEPENDENT RESEARCHER

Private aircraft provide transportation to interesting people: corporate officers, business owners, celebrities, high net-worth individuals, etc.

In recent years, sites like FlightAware have made it trivial to access all public flight plans. However, aircraft owners can opt into a block list (the BARR) that prevents their flight information from being made public. All the interesting people are on the BARR.

We'll explain the basics of how the the ATC system and sites like FlightAware work, demonstrate a serious, unpatchable method for tracking otherwise "untrackable", BARRed aircraft, and demo our site that lets you do the same.

Crypto and the Cops: The Law of Key Disclosure and Forced Decryption

MARCIA HOFMANN
SENIOR STAFF ATTORNEY, ELECTRONIC FRONTIER FOUNDATION

Can the government force you to turn over your encryption passphrase or decrypt your data The law surrounding police attempts to force decryption is developing at breakneck speed, with two major court decisions this year alone. This talk will start off with an in-depth explanation of the Fifth Amendment privilege

PRESENTATIONS

against self-incrimination, its origins, and how it applies to government attempts to force disclosure of keys or decrypted versions of data in the United States. We'll also discuss law enforcement authority to demand passphrases and decryption of data stored with third parties, and survey key disclosure laws in other countries.

Passive Bluetooth Monitoring in Scapy

RYAN HOLEMAN

Recognizing a need to support passive bluetooth monitoring in Scapy, Python's interactive monitoring framework, a project was launched to produce this functionality. Through this functionality, a new means for interactively observing bluetooth was created along with Python APIs to assist in the development of bluetooth auditing, pentesting and exploitation tools.

The project supplements the work of Michael Ossman et al by providing Python extensions and Scapy modules which interact with an Ubertooth dongle. The project also provides support for other passive bluetooth techniques not present in the current Ubertooth core software such as NAP identification, vendor lookup, extended logging and more.

In conjunction with this presentation, the source for this project will be released along with distribution packages for easy installation

Cyber Patriot–A Student's Perspective

KEVIN HOUK, AGE 17
JAKE ROBIE, AGE 18
MATT BRENNER, AGE 18

As the world grows more reliant upon digital technology, cyber-attacks are posing a more significant threat to our nation's security. In recent years, the United States has been falling behind in cyber-related fields. In 2009, the Air Force Association created CyberPatriot, the premiere national high school cyber defense competition, to inspire high school students toward careers in cyber security. In the most recent competition, CyberPatriot IV, 1200 teams competed and were pared down to twelve finalists. Our team from The Marshall Academy placed seventh. Considering the 1200 teams, approximately 7,200, or just about .04%, of high school students participated in this year's CyberPatriot IV. Our goal is to promote Cyber Security at the high school level, in order to better educate future generations in the field. By encouraging greater involvement of both private and public sector organizations, we can bring cyber security to the forefront where it belongs. Currently, CyberPatriot is sponsored by only a few companies, such as Northrop Grumman, Boeing and Microsoft. We believe that by investing in scholarships and grants for cyber security related college degrees, companies can develop the cyber community of tomorrow, and as a result be able to better manage future cyber threats.

How to Hack All the Transport Networks of a Country

ALBERTO GARCIA ILLERA

The presentation is about a real black hacking act against the transport network of a country. It can be extrapolated to any other country. We will show how to get full access to the entire transport network. Manipulating parameters to get free tickets, getting control of the ticket machines, getting clients CC dumps, hooking internal processes to get the client info, pivoting between machines, encapsulating all the traffic to bypass the firewalls, etcetera.

We will show a lot of photos, videos, source code and presentations of the real environment and the skills used to obtain all the information. We will show how combining social engineering and technical skills can be used as a deadly weapon.

Bigger Monster, Weaker Chains: The National Security Agency and the Constitution

JAMEEL JAFFER
DEPUTY LEGAL DIRECTOR, ACLU
WILLIAM BINNEY
FORMER OFFICIAL, NSA
JAMES BAMFORD
INVESTIGATIVE JOURNALIST
ALEX ABDO
STAFF ATTORNEY, ACLU

The National Security Agency, the largest, most powerful spy agency in the world, has taken in an estimated 15 to 20 trillion communications since 9/11, often in defiance of the Constitution and Congressional statutes. The NSA's goal, some say, is to collect virtually all of our electronic communications to allow mass data mining reminiscent of the notorious and now reportedly-defunct program, Total Information Awareness. The limits on the agency's authority to sweep up and analyze this information are critical to our safety and our privacy. The NSA is investing vast amounts in increasing its data storage, code-breaking and analysis capabilities, frequently claiming the investments are for foreign intelligence or "cybersecurity" purposes. However, instead of keeping its equipment trained on terrorism suspects or foreign governments, the NSA is increasingly monitoring the communications of innocent people. Longtime NSA official and whistleblower Bill Binney will join investigative journalist and NSA expert James Bamford and ACLU lawyer Alex Abdo to explore the NSA's goals, reach, and capabilities, and the legality (or illegality) of its actions.

The panel will be moderated by the Deputy Director of the ACLU, Jameel Jaffer.

Black Ops

DAN KAMINSKY
CHIEF SCIENTIST, DKH

If there's one thing we know, it's that we're doing it wrong. Sacred cows make the best hamburgers, so in this year's talk I'm going to play with some techniques that are obviously wrong and evil and naive. There will also be a lot of very interesting code, spanning the range from high speed network stacks to random number engines to a much deeper analysis of non-neutral networks. Finally, we will revisit DNSSEC, both in code, and in what it can mean to change the battleground in your favor.

Owning One to Rule Them All

DAVE KENNEDY
CHIEF SECURITY OFFICER
DAVE DESIMONE
MANAGER, INFORMATION SECURITY

As penetration testers, we often try to impact an organization as efficient and effective as we can to simulate an attack on an organization. What if you could own one system to own them all? That's it, one system. It's all you need, it's in every company, and as soon as you compromise it, the rest fall (no not a domain controller). This presentation will cover a recent penetration test where I came up with a unique avenue to getting over 13,000 shells in just a few minutes by popping one server. I'll be releasing some custom tools to make this simplistic and automate the majority of what was used on this attack. Let's pop a box.

Detecting Reflective Injection

ANDREW KING
CONTRACT RESEARCHER, GRAYHAT RESEARCH, LLC

This talk will focus on detecting reflective injection with some mildly humorous notes and bypassing said protections until vendors start actually working on this problem. It seems amazing that reflective injection still works. Why is that? Because programmers are lazy. They don't want to write new engines, they want to write definitions for an engine that already exists. So what do we do about it? Release a $5 tool that does what $50 AV has failed epically at for several years now., oh and it took me a week or so...Alternately, you could license it to vendors since their programmers are lazy.

An Inside Look Into Defense Industrial Base (DIB) Technical Security Controls: How Private Industry Protects Our Country's Secrets

JAMES KIRK
SENIOR SECURITY CONSULTANT, RAPID7, INC.

With an ever changing threat of nation states targeting the United States and its infrastructure and insiders stealing information for public release, we must continuously evaluate the procedural and technical controls we place on our national assets. This presentation goes into brief detail on how security controls are developed, reviewed, and enforced at a national level for protection of data classified up to Top Secret and some of the major flaws in the security approach to data privacy.

No More Hooks: Trustworthy Detection of Code Integrity Attacks

XENO KOVAH
THE MITRE CORPORATION
COREY KALLENBERG
THE MITRE CORPORATION

Hooking is the act of redirecting program control flow somewhere other than it would go by default. For instance code can be "inlined hooked" by rewriting instructions to unconditionally transfer to other code. Or code can be hooked by manipulating control flow data like function pointers (IAT, IDT, SSDT, return addresses on the stack, callback addresses in dynamically allocated objects, etc). Hooking as a technique is neutral, but it is often used by malicious software to monitor or hide information on a system.

No More Hooks: Trustworthy Detection of Code Integrity Attacks

XENO KOVAH
THE MITRE CORPORATION
COREY KALLENBERG
THE MITRE CORPORATION

Hooking is the act of redirecting program control flow somewhere other than it would go by default. For instance code can be "inlined hooked" by rewriting instructions to unconditionally transfer to other code. Or code can be hooked by manipulating control flow data like function pointers (IAT, IDT, SSDT, return addresses on the stack, callback addresses in dynamically allocated objects, etc). Hooking as a technique is neutral, but it is often used by malicious software to monitor or hide information on a system.

Memory integrity verification requires the ability to detect unexpected hooks which could be causing software to lie or be blinded to the true state of the system. But we don't want to make the same mistake that most security software makes, assuming that they can rely on some built in access control to keep malice at arms length. The history of exploits is the history of bypassing access control. We want to have a technique which can detect if we ourselves are being manipulated to lie even when the attacker is assumed to be at the same high privilege level as our software.

We believe that such a goal can be achieved with the help of an academic technique known as software-based, or timing-based, remote attestation. This is a technique which does not require a hardware root of trust like a TPM in order to bootstrap an ephemeral dynamic root of trust for measurement. It does this by computing a randomized checksum over its own memory and other system state, to detect code or control flow integrity attacks. The self-checking software can still be forced to lie and report an unmodified system, but thanks to a special looping construction, code which causes it to lie will require extra instructions per loop. The extra instructions will be multiplied by the number of loops, causing a macroscopic, remotely-detectable, increase in the runtime vs. what's expected. So basically, an attacker can force our software to lie, but because there's a timing side-channel built into the computation, he can still be caught by taking too long to generate a convincing lie. We have independently implemented and confirmed the claims of past work, and furthermore showed that the timing discrepancy in the presence of a checksum-forging attacker is detectable not just for machines on the same ethernet segment, but over 10 links of our production LAN. Because of the results of other work in timing side-channel detection over internet-scale distances, we think this technique can be extended even further. But for now for longer distances, we use this same timing-based technique in concert with TPM as a trustworthy timer, so that network jitter is not an issue.

DDoS Black and White 'Kungfu' Revealed

ANTHONY 'DARKFLOYD' LAI
SECURITY RESEARCHER, VXRL
TONY 'MT' MIU
KELVIN 'CAPTAIN' WONG
ALAN 'AVENIR' CHUNG
RESEARCHERS, VXRL

Enterprises currently dump millions of bucks to defense against DDoS, some trading firms here are paying for fear to the DDoS attack from China about 5K to 100K USD per day and InfoSec teams believe their solutions are perfect already.

Are those controls effective and unbreakable? In the first part of the presentation, we would like to show our studies and carry out over 10 types of DDoS test against various big firms and organizations to see whether their defense is effective, showing how stupid and smart they are. Various interesting case studies will be briefed :)

In the second part of the presentation, we will detail our proposed defense model to against Application-Level attacks. We have already checked with other vendors and researchers about our model, it is still not yet deployed and hopefully we could put this as an open source project in the future.)

NFC Hacking: The Easy Way

EDDIE LEE
SENIOR SECURITY RESEARCHER, BLACKWING INTELLIGENCE

Until now, getting into NFC/RFID hacking required enthusiasts to buy special hardware and learn about the underlying transfer protocols. No longer! NFCProxy is a new tool (being released at DEF CON 20) that allows you to proxy RFID transactions using Android phones. NFCProxy can record and replay RFID transactions from the perspective of the tag or the PCD (proximity coupling device). NFCProxy is an open source tool/framework that can be used to analyze 13.56?MHz RFID protocols and launch replay (and potentially man in the middle) attacks. You can even use NFCProxy as a virtual wallet by storing previously scanned RFID enabled credit cards and replaying them later at a POS (point of sale) terminal. No fancy equipment needed...just two NFC capable Android phones running ICS (one with a custom rom). Owning RFID enabled credit cards just got easier!

PRESENTATIONS

Robots: You're Doing It Wrong 2

KATY LEVINSON
DIRECTOR OF DEVELOPMENT, HACKER DOJO

By popular demand, DEF CON's angry little roboticist is back with more stories of robot designs gone awry that make practical lessons on making better robots. Drinking will happen: vodka-absconding scoundrels are not invited.

This talk will cover material assuming the average audience member is a relatively intelligent coder with a high-school physics/math background and has seen linear algebra/calculus before. The intent is to navigate people new to robotics around many lessons my teams and I learned the "hard way," and to introduce enough vocabulary for a self-teaching student to bridge the gap between amateur and novice professional robotics. It will not cover why your Arduino doesn't work when you plugged your USB tx into your RS232 tx.

Anonymous and the Online Fight for Justice

AMBER LYON
INDEPENDENT INVESTIGATIVE JOURNALIST
GABRIELLA COLEMAN
CHAIR IN SCIENTIFIC AND TECHNOLOGICAL LITERACY, MCGILL UNIVERSITY, DEPARTMENT OF ART HISTORY & COMMUNICATION STUDIES
MARCIA HOFMANN
SENIOR STAFF ATTORNEY, EFF
MERCEDES HAEFER
STUDENT, UNLV
JAY LEIDERMAN
ATTORNEY, LEIDERMAN DEVINE LLP
GRÁINNE O'NEILL
COORDINATOR ANONLG PROJECT, NATIONAL LAWYERS GUILD

How the media mischaracterizes, & portrays hackers. IRL protest VS. online protest. Politically motivated prosecution. COINTELPRO. The future of hacking and what law enforcement agencies plan to do about it.

OPFOR 4Ever

TIM MALETIC
SENIOR SECURITY CONSULTANT, TRUSTWAVE SPIDERLABS
CHRISTOPHER POGUE
MANAGING CONSULTANT, TRUSTWAVE SPIDERLABS

Training utilizing Opposing Forces, or OPFOR, is an exercise focused on improving detection and response through the principle of "train as you fight." We will demonstrate how we have applied OPFOR to build a continuous feedback loop between penetration testing and incident response. In OPFOR 4Ever, the defense trains the offense just as much as the offense trains the defense, and the exercise has no end date. Come see us demonstrate some attacks as seen from the point of view of the defender as well as the attacker. You can then watch the replay as we use OPFOR principles to evolve these attacks to a form more suitable for real-world penetration testing, pentesting that strives to better simulate what blackhats actually do. This of course raises the bar for incident responders. Evolve or die.

Weaponizing the Windows API with Metasploit's Railgun

DAVID 'THELIGHTCOSINE' MALONEY
SOFTWARE ENGINEER, METASPLOIT – RAPID7

No part of the Metasploit Framework has been shrouded in more mystery and confusion than the Railgun extension. Railgun is one of the most powerful tools in the Metasploit arsenal when it comes to Post Exploitation. In this talk we will examine what Railgun is, and how we can use it to turn Windows completely against itself by weaponizing the Windows API libraries. We will demystify Railgun by explaining exactly how it works under the covers and how you can use it to create powerful post modules.

Defeating PPTP VPNs and WPA2 Enterprise with MS-CHAPv2

MOXIE MARLINSPIKE
DAVID HULTON
MARSH RAY

MS-CHAPv2 is an authentication and key negotiation protocol that, while old and battered, is still unfortunately deployed quite widely. It underpins almost all PPTP VPN services, and is relied upon by many WPA2 Enterprise wireless deployments. We will release tools that definitively break the protocol, allowing anyone to affordably decrypt any PPTP VPN traffic or CHAPv2-based WPA2 handshake with a 100% success rate.

Don't Stand So Close To Me: An Analysis of the NFC Attack Surface

CHARLIE MILLER
PRINCIPAL RESEARCH CONSULTANT, ACCUVANT LABS

Near Field Communication (NFC) has been used in mobile devices in some countries for a while and is now emerging on devices in use in the United States. This technology allows NFC enabled devices to communicate with each other within close range, typically a few centimeters. It is being rolled out as a way to make payments, by using the mobile device to communicate credit card information to an NFC enabled terminal. It is a new, cool, technology. But as with the introduction of any new technology, the question must be asked what kind of impact the inclusion of this new functionality has on the attack surface of mobile devices. In this paper, we explore this question by introducing NFC and its associated protocols. Next we describe how to fuzz the NFC protocol stack for two devices as well as our results. Then we see for these devices what software is built on top of the NFC stack. It turns out that through NFC, using technologies like Android Beam or NDEF content sharing, one can make some phones parse images, videos, contacts, office documents, even open up web pages in the browser, all without user interaction. In some cases, it is even possible to completely take over control of the phone via NFC, including stealing photos, contacts, even sending text messages and making phone calls. So next time you present your phone to pay for your cab, be aware you might have just gotten owned.

How to Hack VMware vCenter Server in 60 Seconds

ALEXANDER MINOZHENKO
SENIOR PENETRATION TESTER, ERPSCAN

This talk will discuss some ways to gain control over the virtual infrastructure through vCenter's services. I will describe a few non-dangerous bugs (they were 0-days when we found them), but if we can use all of them together, we will get administrative access to vCenter which means to the whole virtual network.

DEF CON Comedy Jam V, V for Vendetta

DAVID MORTMAN
CHIEF SECURITY ARCHITECT, ENSTRATUS
RICH MOGULL
SECUROSIS
CHRIS HOFF
RATIONAL SECURITY
DAVE MAYNOR
ERRATA
LARRY PESCE
PAULDOTCOM.COM
JAMES ARLEN
LIQUID MATRIX

You know you can't stay away! The most talked about panel at DEF CON! Nearly two hours of non-stop FAIL. 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 the food cooked on stage to survive. Nothing is sacred not even each other. This years fail includes cloud, mobile and apt to name just a few topics. If that's not enough, we'll also be making crepes on stage. Over the last two years, we've raised over $1,500 for the EFF, let's see how much we can do this year...

Cortana: Rise of the Automated Red Team

RAPHAEL MUDGE
PRINCIPAL, STRATEGIC CYBER LLC

Meet Cortana, a new scripting language to automate Metasploit and extend Armitage. Cortana is a penetration tester's scripting language inspired by scriptable IRC clients and bots. Its purpose is two-fold. You may create long running bots that simulate virtual red team members, hacking side-by-side with you. You may also use it to extend the Armitage GUI for Metasploit. To prevent self-aware bots from taking over the world, Cortana has blanket safety features to provide positive control when enabled. This talk will introduce Cortana, the automation gap it fills, and its capabilities to you. You will see several demonstrations of Cortana in action and get a flavor of what's now possible. Cortana was developed through DARPA's Cyber Fast Track program.

Making Sense of Static - New Tools for Hacking GPS

FERGUS NOBLE
COLIN BEIGHLEY

Current GPS receivers found in mobile phones etc. are capable of about 5m accuracy but high-end receivers costing thousands can get this down to centimeters just using some more sophisticated algorithms and processing. This really opens up a lot of opportunities for UAVs and Quadcopters (and other applications we haven't even thought of – what would you use it for?) and we would like to see this level of performance available in an open-source system.

We have developed and would like to share with you a new set of tools which we hope will make GPS accessible to hackers and experimenters; a library, libswiftnav, which contains a complete toolset for building a GPS receiver, and Piksi, a stand-alone hardware platform to run it on. The prototype is already very capable – we can't wait to see what you can come up with.

SQL ReInjector – Automated Exfiltrated Data Identification

JASON A. NOVAK
ASSISTANT DIRECTOR, DIGITAL FORENSICS, STROZ FRIEDBERG, LLC
ANDREA (DREA) LONDON
DIGITAL FORENSIC EXAMINER, STROZ FRIEDBERG, LLC

This presentation will debut SQL ReInjector, a tool for the rapid assessment of logs from SQL injection attacks to determine what data was exfiltrated.

When responding to an SQL injection attack, responders have to determine what was exfiltrated by manually parsing the web server logs from the victimized host. This is a time consuming process that requires a significant amount of a responder's time. Moreover, manual replay of the SQL injection does not account for system level discrepancies in how queries are executed by the system – running SQL against a SQL server directly doesn't account for the behavior of any intermediary systems – e.g. any application layer logic or nuances in how the web application and database server interact.

SQL ReInjector uses the log files from the machine that has been subject to a SQL injection attack to replay the attack against the server (or a virtualized forensic image thereof) and captures the data returned by the SQL injection web site requests, reducing the amount of time responders have to spend looking at web server logs and allows for responders to recreate the data exfiltrated through a SQL injection attack.

Meet the EFF

KURT OPSAHL
SENIOR STAFF ATTORNEY, EFF
MARCIA HOFMANN
SENIOR STAFF ATTORNEY, EFFF
HANNI FAKHOURI
STAFF ATTORNEY, EFF
PETER ECKERSLEY
DIRECTOR OF TECHNOLOGY PROJECTS , EFF
EVA GALPERIN
INTERNATIONAL FREEDOM OF EXPRESSION COORDINATOR, EFF
TREVOR TIMM
ACTIVIST

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.

The End of the PSTN As You Know It

JASON OSTROM
SECURITY RESEARCHER, VIPER LAB, AVAYA, INC.
JKARL FEINAUER
VULNERABILITY RESEARCH SOFTWARE ENGINEER, VIPER LAB
WILLIAM BORSKEY
SENIOR SECURITY CONSULTANT, VIPER LAB

In this talk, we will explore the so-called market buzz of "UC Federation". Rather, we will kick this term to the bit bucket, and present an overview of how the industry is deploying these solutions technically. We will take a closer look at the security of being able to use UC between organizations, advertised using DNS, the same way that companies use UC internally for VoIP, HD Video, data sharing, IM & Presence, and collaboration applications. This talk is divided into three sections.

First, we'll share our research on the state of public SIP peering using DNS SRV. Is SIP peering proliferating? How? What does it mean? Using a PoC research tool, we'll look at some initial data we've found, in order to plot the increase of peering using DNS SRV records for SIP service location advertisement.

Second, we will show the audience findings from our UC "Federation" Honeypot research project. We've built a UC solution using a large commercial vendor, and have tested "Federation" with the help of the Global Federation Directory. Just to see what would happen. We've also set up a network of cloud based UC Federation honeypots using open source software, to explore attacks against UC Federation Systems.

Last, we show it can be done and how. Did you know that you can set up your own VoIP server with DNS based routing and HA and directly peer between VoIP servers, providing services for your friends and your company from your favorite BYOD using an address just like your email address, right now? For little to no cost, using open source software? It's interesting that when companies communicate VoIP inter-domain, the most prevalent architecture is to route calls over a private network, or through a carrier connected to the PSTN. Ironically, the infrastructure has existed for years to do direct public SIP peering. We'll explore this concept of "Islands of VoIP", and bring together our security research findings in this area along with industry roadblocks. Can a more open standard protocol be adopted using existing

PRESENTATIONS

open source software, to easily UC "Federate" between different vendors? We think this is the future. It's exciting, and we want to show it to you.

APK File Infection on an Android System

BOB PAN
MOBILE SECURITY RESEARCH ENGINEER, TRENDMICRO INC.

This concept of APK file infection on Android is similar to the concept of PE file infection on Windows systems. As the performance of Android device has increased, it's become possible to implement such a concept in Android systems. We will demonstrate how to implement this concept. In addition, we will also give a demo to show that a PoC virus can infect normal APK files in a real Android mobile phone.

Panel: The Making of DEF CON 20

DEF CON DEPARTMENT HEADS

Have you ever wondered what it takes to put DEF CON together, Well now is your chance to find out. DEF CON is broken down into 10 departments: Security, Networking, Press, Speaker Ops, Contests, Vendors, Swag Booth, Registration, Quarter Master, and Operations. Each of the department heads (aka the DEF CON Planning Staff) will be part of this panel and will give an overview of what we do the other 361 days of the year to plan DEF CON. There will also be time for Q&A from the audience so if you want to know how we do this, come prepared with questions.

Anti-Forensics and Anti-Anti-Forensics: Attacks and Mitigating Techniques for Digital-Forensic Investigations

MICHAEL PERKLIN

Digital investigations may be conducted differently by various labs (law enforcement agencies, private firms, enterprise corporations) but each lab performs similar steps when acquiring, processing, analyzing, or reporting on data. This talk will discuss techniques that criminals can use to throw wrenches into each of these steps in order to disrupt an investigation, and how they can even force evidence to be excluded from litigation. Each of these techniques can be detected early by an investigator who is aware of them, and they can be avoided if you know what to look for. Come learn about Anti-Forensic techniques, and the Anti-Anti-Forensic techniques that mitigate them.

Creating an A1 Security Kernel in the 1980s (Using 'Stone Knives and Bear Skins')

TOM PERRINE
SR ENTERPRISE ARCHITECT, SR MANAGER IT INFRASTRUCTURE

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 A1 security-kernel operating system. KSOS was written to protect SCI/compartmented data (sometimes referred to as "above TOP SECRET"), and entered production. KSOS-11 ran on PDP-11, and KSOS-32 ran on DEC VaX. KSOS-11 ran in less than 64K bytes and was a fully functional OS including a security kernel, UNIX compatibility layer and first generation TCP/IP stack.

The design for KSOS was the first operating system design that was mathematically "proven correct" using formal specifications and computer based theorem provers.

The presentation also discusses the computing technology of the day – 16 bit computers, line editors, primitive (by current standards) compilers, theorem provers and how that affected development methods and what could be accomplished.

This presentation is a technical retrospective of computer security research during 1983 – 1090 placed in its social and technical context. This presentation is being written especially for DEF CON's 20th anniversary and has never been published before. The last paper published specifically on KSOS was at the 7th NBS Computer Security Conference in 1984.

Network Anti-Reconnaissance: Messing with Nmap through Smoke and Mirrors

DAN 'ALTF4' PETRO
SECURITY RESEARCHER, DATASOFT CORP.

Reconnaissance on a network has been an attacker's game for far too long, where's the defense? Nmap routinely evades firewalls, traverses NATs, bypasses signature based NIDS, and gathers up the details of your highly vulnerable box serving Top Secret documents. Why make it so easy?

In this talk, we will explore how to prevent network reconnaissance by using honeyd to flood your network with low fidelity honeypots. We then discuss how this lets us constrain the problem of detecting reconnaissance such that a machine learning algorithm can be effectively applied. (No signatures!) We will also discuss some important additions to honeyd that we had to make along the way, and perform a live demonstration of our free software tool for doing all of the above: Nova.

Bypassing Endpoint Security for $20 or Less

PHIL POLSTRA
COMPUTER SECURITY PROFESSOR, UNIVERSITY OF DUBUQUE

In this talk cheap easily constructed devices which can be used to bypass endpoint security software by making any USB mass storage (flash or hard) drive appear as authorized devices will be presented.

The design and implementation will be discussed in detail. Devices can be constructed for approximately $18 and $30 for a small package which requires soldering of 4 wires, and a slightly larger package which requires no soldering, respectively. Some familiarity with microcontrollers and C programming would be helpful, but not required for attendees to get the most from this talk.

The Safety Dance – Wardriving the Public Safety Band

ROBERT PORTVLIET
FOUNDSTONE
BRAD ANTONIEWICZ
FOUNDSTONE

The 4.9Ghz Public Safety Band has been deployed to a town near you! Police, Emergency Medical, and even Critical Infrastructure (power plants, etc.) maintain wireless networks on this seemingly 'hidden' band – but what's actually there? How can you identify and monitor these networks? Stop by and find out the answers to those questions and more!

Kevin Poulsen Answers Your Questions

KEVIN POULSEN

Hacker + Airplanes = No Good Can Come Of This

RENDERMAN
CHIEF RESEARCHER

What happens when a hacker gets bored and starts looking at an aircraft tracking systems? This talk will look at ADS-B (Automatic Dependent Surveillance-Broadcast), a common technology installed or being installed on a vast majority of commercial airliners that involves an unencrypted and unauthenticated radio broadcast. This technology has some interesting features and weaknesses that are a useful lesson in failures when security is not built in from the beginning. This talk constitutes a work in progress and hopes to spur more research and investigation into this field.

MegaUpload: Guilty or Not Guilty?

JIM RENNIE
ATTORNEY
JENNIFER GRANICK
ATTORNEY

On January 19, 2012, Kim DotCom was arrested in a dramatic raid after being indicted on federal criminal charges that he knew that his website, MegaUpload, was a haven of piracy and counterfeiting. In the days that followed, the media commented on the presumed guilt of MegaUpload. In this debate, Jim argues that the law and evidence clearly point to MegaUpload's officers being found guilty, while Jennifer will argue that the MegaUpload case is built on unprecedented and wrongheaded interpretations of copyright law, and thus the principles should be found not guilty. The debate will concentrate on the charges of conspiracy to commit copyright infringement and aiding & abetting copyright infringement. After the arguments and rebuttals, the audience will vote and decide the fate of MegaUpload.

Stamp Out Hash Corruption! Crack All The Things!

RYAN REYNOLDS
MANAGER, SECURITY AND PRIVACY, CROWE HORWATH LLP
JONATHAN CLAUDIUS
SECURITY RESEARCHER, SPIDERLABS RESEARCH, TRUSTWAVE

The precursor to cracking any password is getting the right hash. In this talk we are going to cover how we discovered that Cain and Able, Creddump, Metasploit and other hash extraction tools regularly yield corrupt hashes that cannot be cracked. We will take a deep dive into password extraction mechanics, the birth of a viral logic flaw that started it all and how to prevent corrupt hashes. At the conclusion of this talk we will release patches that prevent hash corruption in these tools that many security professionals use every day.

Spy vs Spy: Spying on Mobile Device Spyware

MICHAEL ROBINSON
CONSULTANT
CHRIS TAYLOR
SECURITY RESEARCHER

Commercial spyware is available for mobile devices, including iPhones, Android Smartphones, BlackBerries, and Nokias. Many of the vendors claim that their software and its operation is undetectable on the smartphones after setup is complete. Is this true? Is there a way to identify whether or not some jerk installed spyware on your mobile phone or are you destined to be PWN'd?

This presentation examines the operation and trails left by five different commercial spyware products for mobile devices. Research for both Android and iPhone 4S will be given. A list of results from physical dumps, file system captures, and user files will be presented to show how stealthy the spyware really was. The results from the analysis of the install files will also be presented. From this information a list of indicators will be presented to determine whether or not spyware is on your phone.

Scylla: Because There's no Patch for Human Stupidity

SERGIO 'FLACMAN' VALDERRAMA
CONSULTING MANAGER, 2SECURE
CARLOS ALBERTO RODRIGUEZ
CO-FOUNDER, 2SECURE

When there's no technical vulnerability to exploit, you should try to hack what humans left for you, and believe me, this always works.

Scylla provides all the power of what a real audit, intrusion, exclusion and analysis tool needs, giving the possibility of scanning misconfiguration bugs dynamically.

Scylla aims to be a better tool for security auditors, extremely fast, designed based on real scenarios, developed by experienced coders and constructed with actual IT work methods.

The words "Configuration Tracer" are the best definition for Scylla, a tool to help on IT audits.

Bruce Schneier Answers Your Questions

BRUCE SCHNEIER

Bruce Schneier will answer questions topics ranging from the SHA-3 competition to the TSA to trust and society to squid.

Programming Weird Machines with ELF Metadata

REBECCA 'BX' SHAPIRO
PHD STUDENT, DARTMOUTH COLLEGE
SERGEY BRATUS
RESEARCH ASSISTANT PROFESSOR, DARTMOUTH COLLEGE

The Executable and Linkable Format (ELF) is omnipresent; related OS and library code is run whenever processes are set up and serviced (e.g., dynamically linked). The loader is the stage manager for every executable. Hardly anyone appreciates the work that the ELF backstage crew (including the linker and the loader) puts in to make an executable run smoothly. While the rest of the world focuses on the star, hackers such as the Grugq (in Cheating the ELF) and Skape (in Locreate: An Anagram for Relocate), and the ERESI/ELFsh crew, know to schmooze with the backstage crew. We can make a star out of the loader by tricking it into performing any computation by presenting it with crafted but otherwise well-formed ELF metadata. We will provide you with a new reason why you should appreciate the power of the ELF linker/loader by demonstrating how specially crafted ELF relocation and symbol table entries can act as instructions to coerce the linker/loader into performing arbitrary computation. We will present a proof-of-concept method of constructing ELF metadata to implement the Turing-complete Brainfuck language primitives and well as demonstrate a method of crafting relocation entries to insert a backdoor into an executable.

We Have You by the Gadgets

MICKEY SHKATOV
TOBY KOHLENBERG
SENIOR INFOSEC SPECIALIST, FORTUNE 500 COMPANY

Why send someone an executable when you can just send them a sidebar gadget? We will be talking about the windows gadget platform and what the nastyness that can be done with it, how are gadgets made, how are they distributed and more importantly their weaknesses. Gadgets are comprised of JS, CSS and HTML and are application that the Windows operating system

PRESENTATIONS

has embedded by default. As a result there are a number of interesting attack vectors that are interesting to explore and take advantage of.

We will be talking about our research into creating malicious gadgets, misappropriating legitimate gadgets and the sorts of flaws we have found in published gadgets.

Can You Track Me Now? Government and Corporate Surveillance of Mobile Geo-Location Data

CHRISTOPHER SOGHOIAN
OPEN SOCIETY FELLOW, OPEN SOCIETY FOUNDATIONS
BEN WIZNER
DIRECTOR, SPEECH, PRIVACY, & TECHNOLOGY PROJECT, ACLU
CATHERINE CRUMP
STAFF ATTORNEY, SPEECH, PRIVACY, & TECHNOLOGY PROJECT, ACLU
ASHKAN SOLTANI
INDEPENDENT RESEARCHER & CONSULTANT ON PRIVACY, SECURITY, AND BEHAVIORAL ECONOMICS

Our mobile phones and apps systematically collect and store comprehensive historical lists of our locations and our travels. Advertising and marketing companies extract and interpret these lists for use in their information-gathering networks, effectively turning our phones into 24/7 location tracking devices. Because this information is readily available to the government, law enforcement agencies now have unparalleled access to knowledge of where you are, where you've been, and through inference, who you are.

In this panel, tech experts Christopher Soghoian and Ashkan Soltani, alongside Catherine Crump, staff attorney with the ACLU's Project on Speech, Privacy, and Technology, will present a briefing on the current technological and legal landscape of location data tracking. The panelists will explore how consumer location tracking efforts weave a story about the systemic privacy vulnerabilities of smart phones and the legal ways in which law enforcement has been able to hitch a ride. The panel will be moderated by the Director of the ACLU's Project on Speech, Privacy, and Technology, Ben Wizner.

Botnets Die Hard – Owned and Operated

ADITYA K. SOOD
SECURITY PRACTITIONER – ISEC PARTNERS | PHD CANDIDATE MICHIGAN STATE UNIVERSITY
RICHARD J. ENBODY
ASSOCIATE PROFESSOR, DEP'T OF COMPUTER SCIENCE AND ENGINEERING, MICHIGAN STATE UNIVERSITY

Botnet designs are becoming more robust and sophisticated with the passage of time. While the security world is grappling with the security threats posed by Zeus and SpyEye, a new breed of botnets has begun to flourish. Present-day botnets such as smoke, ICE-X, NGR, etc use a mix of pre-existing and newly developed exploitation tactics to disseminate infections. Botnets have been successful in bypassing advanced defense mechanisms developed by the industry . This talk will take you to the journey of the lives of present-day botnets. With a good set of demonstrations, we will dissect the crux of upcoming breed of botnets.

How to Channel Your Inner Henry Rollins

JAYSON E. STREET
CIO, STRATAGEM I SOLUTIONS

Have you ever found yourself thinking "Boy I sure wish I could witness a guy rant for 20 minutes and barely come up for air" or maybe "I sure wish I could have seen firsthand an old time tent revival with a preacher screaming at me" Well then great news you are in luck. This is a talk on not just how we need to take a hard look at how we interact with people outside of our field. It also addresses how we can escape the echo chamber and hopefully burn it to the ground as we leave! All presented in a hopefully comical but most likely just ranty way!

Can Twitter Really Help Expose Psychopath Killers' Traits?

CHRIS 'THE SUGGMEISTER' SUMNER
THE ONLINE PRIVACY FOUNDATION
RANDALL WALD
RESEARCHER

Recent research has identified links between Psychopaths and the language they use (Hancock et al 2011), with media reports suggesting that such knowledge could be applied to social networks in order help Law Enforcement Agencies expose "Psychopath killers' traits". This is the first public study to research Psychopathy in the context of social media. Results show that there are a number of statistically significant correlations between an individual's darker personality traits and their Twitter activity. We also identified links between users' attitudes to privacy, their personality traits and their twitter use. We will present the improvement gains possible through the use of machine learning for personality prediction and share the models and techniques employed.

In addition to presenting our results, this talk will provide an introduction into identifying psychopathic traits using the Hare Psychopathy Checklist (PCL-R), present the technical approaches to collecting, storing and analyzing Twitter data using Open Source technologies and discuss the current ethical, privacy and human rights concerns surrounding social media analysis, vetting and labeling.

We will conclude with two proof of concept works, the first using the visualization tool Maltego to explore how visual analysis could be used to identify potential troublemakers at events such a far right demonstrations; the second to look at how personality traits influence response and interaction with a benign Twitter Bot.

.

Attacking the TPM Part 2 : A Look at the ST19WP18 TPM Device

CHRISTOPHER "BIGGUN" TARNOVSKY
OWNER OF FLYLOGIC, INC.

The STMicroelectronics ST19WL18P TPM die-level analysis. Companies like Atmel, Infineon and ST are pushing motherboard manufacturers to use these devices. End-users trust these devices to hold passwords and other secrets. Once more, I will show you just how insecure these devices are.

Twenty Years Back, Twenty Years Ahead: The Arc of DEF CON Past and Future

RICHARD THIEME
THIEMEWORKS

Thieme's keynote at DEF CON 4 for a few hundred people was "Hacking as Practice for Trans-planetary Life in the 21st Century." Mudge recently said, "Some of us knew what you meant, and some of us thought you were nuts." That's likely to be the response to this talk too. Thieme addresses what he said 17 cons ago, why it was true, and illuminates some likely futures for hacking and hackers, anonymous 2.0.1, and the gray space of the noir world in which one is deemed a "criminal," not because of what one does, but according to who one does it for.

Identity, in short, is destiny. More than ever, identity is a choice, modular and fluid.

Mudge was with the l0pht then, now he's with DARPA. Jeff Moss was an entrepreneurial hacker, now's he's with Homeland Defense. Too many to name work in agencies or stateless names and nameless states, fulfilling the vision of Thieme's first speech.

But that was then. What's likely to be next?

Off-Grid Communications with Android: Meshing the Mobile World

JOSH 'MONK' THOMAS
BREAKER OF THINGS, MITRE CORPORATION
JEFF 'STOKER' ROBBLE
MITRE CORPORATION

Join the SPAN team for a deep dive into the Android network stack implementation and its limitations, an analysis of the Wi-Fi chipsets in the current generation of smart phones and a collection of lessons learned when writing your own network routing protocol (or 5 of them). The team will also share a "How To" walkthrough into implementing your own Mesh network and incorporating general "Off Grid" concepts into your next project; this will include securing your mesh from outside parties while tunneling and bridging through the internet. The team will delve into specific Android limitations of Ad-Hoc networking and provide workarounds and bypass mechanisms. Lastly, the team will give an overview of the implementations and network surfaces provided by the new collection of networking alternatives, including NFC and Wi-Fi Direct.

Socialized Data: Using Social Media as a Cyber Mule

THOR (HAMMER OF GOD)
CHIEF DEITY, HAMMER OF GOD

When thinking like a "bad guy" with the goal of distributing any number of covert communications to any number of recipients, there are a number of critical attributes which should be present. The message should:

– Be portable and "self-sustaining.
– Be able to be propagated without the originator actually having to *own* the message or carry it on him.
– Have the ability to control which recipients receive/can read the message.
– Have the messages backed up and managed by a 3rd party in perpetuity.
– Be free
– Be able to be received without any privileged access to equipment or require specialized equipment to receive.
– Be detection resistant, or even detection PROOF.

This session will be about how to go about just that. ALL of these attributes will be satisfied, and I will illustrate how you can literally have a "detection-proof" covert communication. I don't think I've ever said that before, and just writing the words "detection-proof" makes me cringe just a bit. But I've racked my brain on a way to detect what I'll show you and I can't find a way to do it.

That will be the other cool part of this talk – we'll all brainstorm at the end on a way to detect this. I bet you can't. :) To me, this is the epitome of what DEF CON is about, and I hope you'll join me at this talk. Besides, my super-hot wife will be there. Get hammered at Hammer of God!!!

Safes and Containers: Insecurity Design Excellence

MARC WEBER TOBIAS
INVESTIGATIVE ATTORNEY AND SECURITY SPECIALIST, SECURITY.ORG
MATT FIDDLER
SECURITY SPECIALIST, SECURITY.ORG
TOBIAS BLUZMANIS
SECURITY SPECIALIST, SECURITY.ORG

Insecure designs in physical security locks, safes, and other products have consequences in terms of security, liability, and even loss of life. Marc Weber Tobias and his colleagues Tobias Bluzmanis and Matthew Fiddler will discuss a number of cases involving design issues that allow locks and safes to be opened in seconds, focusing on consumer-level containers that are specified as secure for storing valuables and weapons, and in-room hotel safes that travelers rely upon.

In one instance, the insecurity of a consumer gun safe that is sold by major retailers in the United States played a part in the death of a three year old child who was able to gain access to a handgun that was locked in a supposedly secure container.

The presenters will demonstrate different product designs that were represented as secure but in fact are not.

Rapid Blind SQL Injection Exploitation with BBQSQL

BEN TOEWS
SECURITY CONSULTANT, NEOHAPSIS
SCOTT BEHRENS
SECURITY CONSULTANT, NEOHAPSIS

Blind SQL injection can be a pain to exploit. When the available tools work they work well, but when they don't you have to write something custom. This is time-consuming and tedious. This talk will be introducing a new tool called BBQSQL that attempts to address these concerns. This talk will start with a brief discussion of SQL Injection and Blind SQL Injection. It will then segue into a discussion of how BBQSQL can be useful in exploiting these vulnerabilities. This talk will cover how features like evented concurrency and character frequency based searching can greatly improve the performance of a SQL Injection tool. This talk should leave you with enough knowledge to begin using BBQSQL to simplify and speed up your application pentests.

Subterfuge: The Automated Man-In-The-Middle Attack Framework

MATTHEW TOUSSAIN
UNITED STATES AIR FORCE
CHRISTOPHER SHIELDS
UNITED STATES AIR FORCE

Walk into Starbucks, plop down a laptop, click start, watch the credentials roll in. Enter Subterfuge, a Framework to take the arcane art of Man-in-the-Middle Attacks and make it as simple as point and shoot. Subterfuge demonstrates vulnerabilities in the ARP Protocol by harvesting credentials that go across the network, and even exploiting machines through race conditions. Now walk into a corporation...

A rapidly-expanding portion of today's Internet strives to increase personal efficiency by turning tedious or complex processes into a framework which provides instantaneous results. On the contrary, much of the information security community still finds itself performing manual, complicated tasks to administer and protect their computer networks. The purpose of this presentation is to discuss a new Man-In-The-Middle attack tool called Subterfuge. Subterfuge is a simple but devastatingly effective credential-harvesting program, which exploits vulnerabilities in the inherently trusting Address Resolution Protocol. It does this in a way that even a non-technical user would have the ability, at the push of a button, to attack all machines connected to the network. Subterfuge further provides the framework by which users can then leverage

PRESENTATIONS

a MITM attack to do anything from browser/service exploitation to credential harvesting thus equipping information and network security professionals and enthusiasts alike with a sleek "push-button" security validation tool.

Drinking From the Caffeine Firehose We Know as Shodan

VISS
INFORMATION SECURITY CONSULTANT, GENTLEMAN OF FORTUNE

Shodan is commonly known for allowing users to search for banners displayed by a short list of services available over the internet. Shodan can quite easily be used for searching the internet for potentially vulnerable services to exploit, but it's also a powerful defensive posturing tool as well as the first step in aggregating wide scopes of data for mining. Everyone knows routers, switches and servers are connected to the internet – but what else is out there? Has anybody even looked? I suspect people stop after the popular searches and forego what's left. Did you know there are hydrogen fuel cells attached to the internet? Some of my findings were pretty surprising, and these discoveries are an excellent metric for identifying how successful our security campaigns as an industry are. It's a way to measure our success as a whole, by scanning the entire internet.

The DCWG Debriefing - How the FBI Grabbed a Bot and Saved the Internet

PAUL VIXIE
CHAIRMAN AND FOUNDER, INTERNET SYSTEMS CONSORTIUM
ANDREW FRIED
SENIOR CONSULTANT, CUTTER CONSORTIUM'S BUSINESS TECHNOLOGY STRATEGIES AND GOVERNMENT & PUBLIC SECTOR PRACTICES

Shodan is commonly known for allowing users to search for banners displayed by a short list of services available over the internet. Shodan can quite easily be used for searching the internet for potentially vulnerable services to exploit, but it's also a powerful defensive posturing tool as well as the first step in aggregating wide scopes of data for mining. Everyone knows routers, switches and servers are connected to the internet – but what else is out there? Has anybody even looked? I suspect people stop after the popular searches and forego what's left. Did you know there are hydrogen fuel cells attached to the internet? Some of my findings were pretty surprising, and these discoveries are an excellent metric for identifying how successful our security campaigns as an industry are. It's a way to measure our success as a whole, by scanning the entire internet.

The Christopher Columbus Rule and DHS

MARK WEATHERFORD
DEPUTY UNDERSECRETARY FOR CYBERSECURITY FOR THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE (NPPD) AT THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY

"Never fail to distinguish what's new, from what's new to you." This rule applies to a lot people when they think about innovation and technology in the government. At the U.S. Department of Homeland Security, in addition to running the National Cybersecurity and Communication Integration Center (NCCIC), the US-CERT and the ICS-CERT, they work daily with companies from across the globe to share critical threat and vulnerability information. DHS also supports and provides funding for a broad range of cutting-edge cybersecurity research initiatives, from the development and implementation of DNSSEC to sponsoring the use of open source technologies and from development of new cyber forensics tools to testing technologies that protect the nation's industrial control systems and critical infrastructures. This is not your grandfather's Buick! During this presentation Deputy Under Secretary for Cybersecurity Mark Weatherford will talk about research and training opportunities, the growing number of cybersecurity competitions sponsored by DHS, and how they are always looking to hire a few good men and women.

The Art Of The Con

PAUL WILSON
REAL HUSTLER

Paul Wilson is the writer and star of "The Real Hustle" and creator of "The Takedown" on Court TV and "Scammed" on The History Channel. He is one of the world's finest magicians and an expert on cons, scams, casino cheating and gambling sleight of hand. He has pulled more confidence tricks than anyone in history in his efforts to inform and protect the public.

This talk will include a live con game, cheating devices and reasons why people will always be vulnerable.

Improving Web Vulnerability Scanning

DAN ZULLA

A new approach for web vulnerability scanning that outbids most existing scanners.

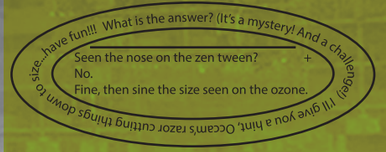
Q&A with the Men (and Women) in Black

PRIEST AND PANEL

Back at DC9 a brave MIB from the CIA received clearance and volunteered to answer any and all DC attendee's questions with no restrictions as honestly as he could. After that experience it's only taken us 10 years to get several someone's to come back and do it again!

This will be your chance to meet and ask any question you want of the so called Men (and Women) in Black. Representatives from the NRO, CIA, NSA, DIA, and US Military will field any and all questions you have on any topic you want. However you may not like the answers.

We promise there will be no extreme renditions, water boarding, assassinations, or mind control unless you really truly deserve it.



DEFCON.ORG

DEF CON Forums

If there's one idea we want all new Con-goers to leave with, it's that DEF CON is a lot more than an annual event. Over the past 20 years, DEF CON has grown into a real global community $. We take pride in getting all these bright, curious and motivated people all in one place to learn, to socialize, and to recalibrate their livers, but we don't want any of it to end on Sunday afternoon.

Fortunately , it doesn't. The DEF CON forums are full of ways to keep your DEF CON experience going until we are all together again in meatspace.

Want to meet other DEF CON fans in your zip code? Every DC Group has a thread in our forum so that you can find out what they're up to. Feel like you need to talk about a presentation you saw here? Want to get involved in a DC event? A lot of the planning goes on in the Forums, too, so if you have [good] ideas, we encourage you to drop in and share them.

Sure, it might be a while unti the next DEF CON, but we've got a nice place to hang until then.

DEF CON Pics

One thing we never get enough of here at DEF CON HQ is pictures of the Con. We love to digitally immortalize the dunk tanks, the toxic BBQs, what have you. And since we couldn't help but notice that most of you are walking around with approximately 2.3 HD-capable digital cameras in your various tactical cargo pockets and backpacks,we'd like to ask for your help. If you take pictures you think are cool of DEF CON events, presentations or just general ambience, please share them with us at pics.defcon.org.

It's wins all around - you get to share your CON memories with the community, we get pictures to use in our projects and some of us will be grateful to know exactly what was going on in the hours they can't ac-count for.

Please note that many DEF CON attendees are camera-shy for a variety of reasons, so etiquette is a must. It's better to ask if someone minds having a picture taken in their airspace than to find out too late that they do.

We look forward to seeing your pics, and archiving them online for posterity.

VENDORS

ACLU

The American Civil Liberties Union of Northern California works 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. ACLU-NC's Demand Your dotRights Campaign highlights the need for modern privacy protections to match the technology we develop and use. We work with users, technologists, businesses, and lawmakers to update legal and practical protections so that users don't have to choose between taking advantage of new technology and losing control of their personal information. Please stop by our booth in the vendor area to learn more about our campaign and what you can do to help!

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. BumpMyLock's sister-site, ACE Hackware, is your premier source for hackware, spy gear, disguises, surveillance and night vision equipment for penetration testing, ethical hacking and social engineering. ACE Hackware was founded by long-time pentester and hacking countermeasures instructor Taylor Banks with the help of a close-knit group of hacker friends who know exactly what you need to perform professional penetration tests, physical security audits and social engineering engagements. 5% of all our sales will go to the Miracle Match Foundation.

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!

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.

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.

HackerStickers.com

HackerStickers.com offers the best in hacker threads, caffeine, technology and mind bending tools for all trades. Official reseller of DEF CON swag after the con!

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.

LBGFX

Customize T shirts & Stickers on the spot at DEF CON 20

MECO

Our 15th year at DEF CON! From Parts and Subassemblies, Test Equipment, and Military Hardware, to Security Equipment, and Fetish Clothing! MECO strives to bring you an eclectic mixture of the finest techno-trinkets.... Stop on by and see us!

Ninja Networks

Ninja Networks returns with their limited edition challenge coins, custom made for DEF CON each year. Once they're gone, they're gone, and never remade. Please note that our most popular designs have always sold out by Saturday. (Note for feds/spooks/etc: We do trade coins. Ask at the booth or track down barkode.)

No Starch Press

No Starch Press is one of the few remaining independent computer book publishers. New for 2012: Practical Malware Analysis, LEGO Heavy Weapons, The Manga Guide to Linear Algebra, The Tangled Web, Ubuntu for Your Mom, Wonderful Life with the Elements, Super Scratch Programming Adventure!, Think Like a Programmer, and more. Stop by for some stickers, maybe a shotglass, other swag, and save 30% on everything.

Null Space Labs

Electronic devices for the modern hacker.

Pwnie Express

Pwnie Express specializes in bleeding edge pentesting hardware, including the first-to-market commercial pentesting dropbox, the Pwn Plug. A full pentesting suite packed into an inconspicuous microserver, the Pwn Plug uses covert tunnels and 3G/GSM cell service to maintain an encrypted, firewall-busting backdoor into your target network. Stop by our booth early as we'll be unveiling TWO NEW PRODUCTS at DEF CON 20!

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, 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, solid Titanium bike lock, $1500 padlock, and a variety of other unique products.

SERE PICK

SEREPICK specializes in custom, covert entry tools and kits for the Urban Penetration Tester. Our flagship product is the Titanium Bogota Entry Toolset which will again be available in various configurations. We will also be offering complete kits including our custom Titanium, Polymer and Ceramic tools.

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! Some extra special items will be available in celebration for 20 years of shaping technology-as-we-know-it!

Simple WiFi

SimpleWiFi specializes in long range WiFi antennas, cables and USB adapters. We manufacture in south Florida most of our antennas and cables as well as quality control on all our products that pass through our doors.

Table of Ample Random Doodads Including Stickers (TARDIS)

Every year we've sold electronics kits – trying to get people more involved with hardware. We will have stickers and other randomness too! Come visit the TARDIS in the vendor area.

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)

MOVIE NIGHT

Watching movies with DT on Friday and Saturday night is a time-honored DEFCON 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!

'21' FRIDAY, 18:00

Join us for a screening of the hit movie "21" and stick around for a Q&A session with "MIT Mike" Aponte, the real-life inspiration for the character "Jason Fisher".

"MIT Mike" Aponte Mike Aponte is a world-renowned blackjack player, gaming consultant and professional speaker. Mike was the leader of the MIT Blackjack Team, a high stakes card-counting team that legally won millions at 21 using mathematics and an ingenious approach. Mike was one of the main characters in the New York Times bestseller, Bringing Down the House, which inspired the major motion picture, 21.

'CODE 2600' FRIDAY, 20:00

We will be the first hacker con to have the film shown and we are pretty excited about it. The filmmaker will be present and doing a Q & A after the screening! Check out code2600.com for more info!

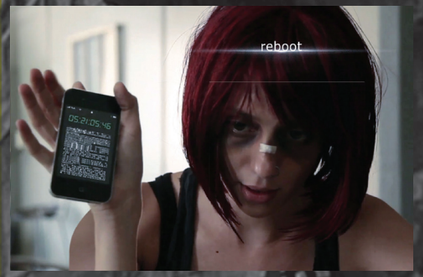
CODE 2600 documents the rise of the Information Technology Age as told through the events and people who helped build and manipulate it. The film explores the impact this new connectivity has on our ability to remain human while maintaining our personal privacy and security. As we struggle to comprehend the wide-spanning socio-technical fallout caused by data collection and social networks, our modern culture is trapped in an undercurrent of cyber-attacks, identity theft and privacy invasion. Both enlightening and disturbing, CODE 2600 is a provocative wake-up call for a society caught in the grips of a global technology takeover.

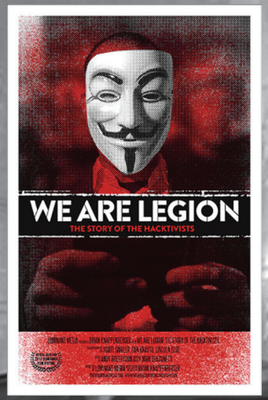
WITH THE DARK TANGENT

'REBOOT' SATURDAY, 19:00

We are very excited to announce an Exclusive Sneak Preview screening of the film Reboot at DEF CON 20! Stay after for Q&A with the filmmakers and cast! Here's a little glimpse into the film:

In contemporary Los Angeles, a young female hacker (Stat) awakens from unconsciousness to find an iPhone glued to her hand and a mysterious countdown ticking away on the display. Suffering from head trauma, and with little recollection of who she is or what is happening, Stat races against time to figure out what the code means, and what unknown event the pending zero-hour will bring.





'WE ARE LEGION' SATURDAY, 21:00

"We Are Legion: The Story of the Hacktivists" is a documentary that takes us inside the world of Anonymous, the radical "hacktivist" collective that has redefined civil disobedience for the digital age. The film explores the historical roots of early hacktivist groups like Cult of the Dead Cow and Electronic Disturbance Theater and then follows Anonymous from 4chan to a full-blown movement with a global reach, one of the most transformative of our time.

We might even get lucky and have some cast and crew in attendance for a short Q&A!

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 1

10:00 **Wireless Security: Breaking Wireless Encryption Keys**
DaKahuna

11:00 **Intro to Digital Forensics: Tools & Tactics**
Ripshy & Jacob

12:00 **Cerebral Source Code**
Siviak

13:00 **DC101: DEF CON Survival**
HighWiz, Lockheed, Runnerup, Roamer, AlxRogan, Pyr0, Flipper

14:00 **Screw the Planet, Hack the Job!**
Roamer, Lockheed, Heather, Alxrogan

15:00 **HF skiddies suck, don't be one. Learn some basic Python.**
Terrence "tuna" Gareau

16:00 **Hacking the Hackers: How Firm is Your Foundation?**
LoST

17:00 **Fun with the Lockpick Village**
Dr. Tran

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 16:30-22:00, Sunset park

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

Excited to be back in its 8th year at Defcon!!

theSummit is a Fundraiser for the Electronic Frontier Foundation (EFF) on Thursday Night between Black Hat, BSides, and DEF CON events. We host this event to offer you the opportunity to meet up with many of this year's

speakers and VIPs. It's not easy to see every talk you want, or to track speakers down when you have a question. Here is your chance get direct access to some of the industry leaders so you can discuss a talk, get advice about a project, or just buy them a beer to say thanks for all the hacks. Open to all ages, theSummit is an excellent networking opportunity with a live auction that often includes keys to some of the contests, a full bar, and entertainment provided by Dual Core & Dale Chase, DJ Jackalope, DJ Sailor Gloom and introducing 8Bit Weapon with their original chip tunes using vintage computers and gaming consoles as instruments. Open Bar sponsored by the Digital Liberation Front (DLF) while supplies last! As always, 100% of our proceeds is donated to the EFF.

theSummit()
`year = 2012;`

Start Time: Thursday, July 26, 2010 at 8:00pm Vegas 2.0: bit.ly/effsummit

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 8Bit Weapon

23:30 Raffle

00:00 DJ Jakalope

00:30 DJ Sailor 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, Nick, Matt, Salem, Cuddles, Astcell, DJ Jackalope, DJ Sailor Gloom, Dual Core, Dale Chase, and of course the people behind the EFF that make us puke rainbows.

FRIDAY JULY 27

	PENN & TELLER	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	**The Christopher Columbus Rule and DHS** Mark Weatherford	**Welcome & Badge Talk** The Dark Tangent, LoST, Jason Scott	**Should the Wall of Sheep Be Illegal?** Kevin Bankston Matt Blaze Jennifer Granick	**Making Sense of Static – New Tools for Hacking GPS** Fergus Noble Colin Beighley	**Embedded Device Firmware Vulnerability Hunting** Ang Cui
					APK File Infection on an Android System Bob Pan
11:00	**Socialized Data: Using Social Media as a Cyber Mule** Thor	**Trailer to the DEF CON Documentary, Intro by Dead Addict and Gail Thackeray** Jason Scott, Dead Addict, Gail Thackeray	**MegaUpload: Guilty or Not Guilty?** Jim Rennie, Jennifer Granick	**Can You Track Me Now? Government And Corporate Surveillance Of Mobile Geo-Location Data** Christopher Soghoian, Ben Wizner, Catherine Crump, Ashkan Soltani	**Passive Bluetooth Monitoring in Scapy** Ryan Holeman
					Not-So-Limited Warranty Darkred
12:00	**Cortana: Rise of the Automated Red Team** Raphael Mudge	**Shared Values, Shared Responsibility** General Keith B. Alexander	**Meet the EFF** Kurt Opsahl, Marcia Hoffman, Hanni Fakhouri, Peter Eckersley, Eva Galperin, Trevor Tim		**Not So Super Notes** Matthew Duggan
					The Open Cyber Challenge Platform Project Linda C. Butler
13:00	**Owning One to Rule Them All** Dave Kennedy, Dave Desimone	**The Art of Cyberwar** Kenneth Geers	**Panel: The Making of DEF CON 20** DEF CON Department Heads	**Don't Stand So Close To Me: An Analysis of the NFC Attack Surface** Charlie Miller	**How to Channel Your Inner Henry Rollins** Jayson E. Street
					Bad (and Sometimes Good) Tech Policy: It's Not Just a DC Thing Chris Conley
14:00	**Changing the Security Paradigm: Taking Back Your Network and Bringing Pain to the Adversary** Shawn Henry	**Drones!** Chris Anderson	**Crypto and the Cops: the Law of Key Disclosure and Forced Decryption** Marcia Hofmann	**NFC Hacking: The Easy Way** Eddie Lee	**Scylla: Because There is No Patch for Human Stupidity** Sergio Valderrama, Carlos Rodriguez
					Drinking From the Caffeine Firehose We Know as Shodan Viss
15:00	**Detecting Reflective Injection** Andrew King	**An Inside Look Into Defense Industrial Base (DIB) Technical Security Controls: How Private Industry Protects Our Country's Secrets** James Kirk	**Panel: DEF CON Comedy Jam V, V for Vendetta** David Mortman, Rich Mogull, Chris Hoff, Dave Maynor, Larry Pesce, James Arlen	**Attacking the TPM Part 2 : A look at the ST19WP18 TPM device** Christopher Tarnovsky	**Network Anti-Reconnaissance** Dan 'AltF4' Petro
					How to Hack VMware vCenter Server in 60 Seconds Alexander Minozhenko
16:00	**Post-Exploitation Nirvana: Launching OpenDLP Agents over Meterpreter Sessions** Andrew Gavin, Michael Baucom, Charles Smith	**Life Inside a Skinner Box: Confronting our Future of Automated Law Enforcement** Greg Conti, Lisa Shay, Woodrow Hartzog		**Bypassing Endpoint Security for $20 or Less** Phil Polstra	**Demorpheos** Svetlana Gaivoronsli, Denis Gamayunov
					New Techniques in SQLi Obfuscation Nick Galbreath
17:00		**Anti-Forensics and Anti-Anti-Forensics: Attacks and Mitigating Techniques for Digital-Forensic Investigations** Michael Perklin	**The Art of the Con** Paul Wilson	**Safes and Containers – Insecurity Design Excellence** Marc Weber Tobias, Matt Fiddler, Tobias Bluzmanis	**DivaShark – Monitor Your Flow** Robert Deaton
					Blind XSS Adam Baldwin

SATURDAY JULY 28

	Penn & Teller	Track 1	Track 2	Track 3	Track 4
10:00	**Defeating PPTP VPNs and WPA2 Enterprise with MS-CHAPv2** Moxie Marlinspike, David Hulton, Marsh Ray	**Twenty Years Back, Twenty Years Ahead: The Arc of DEF CON Past and Future** Richard Thieme	**World War 3.0 – The battle for the Internet between the forces of Chaos & Control** Joshua Corman, Dan Kaminsky, Jeff Moss, Rod Beckstrom, Michael Joseph Gross	**Beyond the War on General Purpose Computing: What's Inside the Box?** Cory Doctorow	**Creating an AI Security Kernel in the 1980s (Using "Stone Knives and Bear Skins")** Tom Perrine
11:00	**Stamp Out Hash Corruption! Crack All The Things** Ryan Reynolds, Jonathan Claudius	**Hacking Humanity: Human Augmentation and You** Christian 'Quaddi' Dameff Jeff 'r3plicant' Tully	**Bruce Schneier Answers Your Questions** Bruce Schneier	**Owning Bad Guys {And Mafia} With Javascript Botnets** Chema Alonso, Manu 'The Sur'	**Exploit Archaeology: Raiders of the Lost Payphones** Josh Brashars
12:00	**Cryptohaze Cloud Hacking** Bitweasil	**DIY Electric Car** David Brown	**Meet the Fed Panel One** Jim Christy, Leon Carroll, Andy Fried, Jon Iadonisi, Rich Marshall, david McCallum, Justin Wykes	**Botnets Die Hard – Owned and Operated** Aditya K. Sood, Richard J. Enbody	**Into the Droid: Gaining Access to Android User Data** Thomas Cannon
13:00	**The End of the PSTN As You Know It** Jason Ostrom, Karl Feinauer, William Borskey	**More Projects of Prototype This!** Joe Grand, Zoz	**Meet the Fed Panel Two** Jim Christy, Rod Beckstrom, Jerry Dixon, Mishel Kwon, Bob Lentz, Riley Repko, Dr. Linton Wells, Mark Weatherford	**Hardware Backdooring is Practical** Jonathan Brossard	**Hellaphone: Replacing the Java in Android** John Floren
14:00	**Programming Weird Machines with ELF Metadata** Rebecca 'bx' Shapiro, Sergey Bratus	**<ghz or Bust: DEF CON** Atlas	**Q&A with the Men (and Women) in Black** Priest, others	**Hacking Measured Boot and UEF** Dan Griffin	**Off Grid Communications with Android – Meshing the Mobile World** m0nk, Stoker
15:00	**Uncovering SAP Vulnerabilities: Reversing and Breaking the Diag Protocol** Martin Gallo	**The Safety Dance – Wardriving the Public Safety Band** Robert Portvliet, Brad Antoniewicz	**Bigger Monster, Weaker Chains: The NSA and the Constitution** Jameel Jaffer, William Binney, James Bamford, Alex Abdo	**DDoS Black and White "Kungfu" Revealed** Anthony 'Darkfloyd' Lai, Tony 'MT' Miu, Kelvin 'Captain' Wong, Alan 'Avenir' Chung	**Exchanging Demands** Peter Hannay
16:00	**Black Ops** Dan Kaminsky	**Hacker + Airplanes = No Good Can Come Of This** Renderman	**Connected Chaos: Evolving the DCG/Hackspace Communication Landscape** blakdayz, anarchy angel, anch, Dave Marcus, Nick Farr	**(BSDaemon) Overwriting the Exception Handling Cache Pointer – Dwarf Oriented Programming** Rodrigo Branco, Sergey Bratus, James Oakley	**Spy vs. Spy: Spying on Mobile Device Spyware** Michael Robinson, Chris Taylor
17:00		**Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit** Dustin Hoffman, Semon Rezchikov	**Panel: Anonymous and the Online Fight for Justice** Amner Lyon, Gabriella Coleman, Marcia Hofmann, Mercedes Haefer, Jay Leiderman, Gráinne O'Neill	**The DCWG Debriefing – How the FBI Grabbed a Bot and Saved the Internet** Paul Vixie, Andrew Fried	**The Darknet of Things, Building Sensor Networks That Do Your Bidding** Anch, Omega

DEF CON GROUPS

You know that hollow feeling you get on the last day of DEF CON?

The awards ceremony is over, the vendors are packing it in, the lobby is full of people checking out and heading for the airport. You're thinking about going back to work, about finding yourself away from the tribe and back among the Normals. Makes you wish DEF CON was going on all year, right?

The good news is, DEF CON _is_ going on all year, and in generally more forgiving weather. There are DC Groups all over the world. All of them have monthly meetings where they discuss some meaty technical topic. Some of them have hackerspaces,and cool projects. Some of them bring in speakers and try to keep the info-sharing going on for the 361 days when the CON is dark.

If you're not linked up with your local DC group, you owe it to yourself to get familiar. Interesting people talking about interesting tech and bending it to interesting purposes, what more could you conceivably require? I mean, it's not like you're gonna have more fun at the Elks lodge. No one teaches you to pick locks at Kiwanis Club. To find out if you've got a local DC group, check the listing on the DEF CON site (https://www.defcon.org/html/DEF CON-groups/dc-groups-index.html)

If your town doesn't have a DC group yet, you should consider starting one. We make it pretty easy. Fill out the form at http://goo.gl/hqGQ3, and we'll get back to you with your status. Find a place that doesn't mind you hanging out and talking a bit — libraries can work, parks can work, that cool back room at your local caffeine dispensary, even. Maybe not your creepy unfinished basement, but there really are almost endless options. Maybe even throw up a website to keep track of everything. You get the cool points for starting the group, and when it turns awesome you get to make the biggest awesome face.

The best thing about lugging around these giant craniums is that we don't have to discover everything ourselves. We can learn from each other. Intentional knowledge sharing is a force multiplier, and it's the thing that moves the world forward. If you have cool ideas (and if you didn't, you probably wouldn't be reading this) then do your part for a better tomorrow and start sharing them. If you know other smart people who need an audience, or who just want to get smarter, invite them in.

It's pretty win-win. You keep learning and sharing what you do with us, and we'll keep looking for ways to shine a light on all the cool happenings in DCG-land. Let's make the Geek Christmas feeling of DEF CON last all year long.

SUNDAY JULY 29

	Track 1	Track 2	Track 3	Track 4
10:00	**SIGINT and Traffic Analysis for the Rest of Us** Sandy Clark, Matt Blaze	**Robots: You're Doing it Wrong 2** Katy Levinson	**Trustwave, OPFOR 4Ever** Tim Maletic, Christopher Pogue	**We Have You by the Gadgets** Mickey Shkatov, Toby
11:00	**SCADA Strangelove or: How I Learned to Start Worrying and Love the Nuclear Plants** Sergey Gordeychik, Denis Baranov, Gleb Gritsai	**KinectasploitV2: Kinect Meets 20 Security Tools** Jeff Bryner	**Improving Web Vulnerability Scanning** Dan Zulla	**No More Hooks: Trustworthy Detection of Code Integrity Attacks** Xeno Kovah, Corey Kallenberg
12:00	**Looking into the Eye of the Meter** Cutaway	**Cyber Patriot – A Student's Perspective** Kevin Houk, Matt Brenner, Jake Robie	**Post Metasploitation: Improving Accuracy and Efficiency in Post Exploitation Using the Metasploit Framework** egypt	**Owning the Network: Adventures in Router Rootkits** Michael Coppola
13:00	**Tenacious Diggity – Skinny Dippin in a Sea of Bing** Francis Brown, Rob Ragan	**DC Recognize Awards** Jeff Moss, Jericho, Russ Rogers	**Weaponizing the Windows API with Metasploit's Railgun** David 'thelightcosine' Maloney	**Hacking [redacted] Routers** FX, Greg
14:00	**Can Twitter Really Help Expose Psychopath Killers' Traits?** Chris "The Suggmeister" Sumner	**Fuzzing Online Games** Elie Bursztein, Patrick Samy	**Kevin Poulsen Answers Your Questions** Kevin Poulsen	**SQL Injection to MIPS Overflows: Rooting SOHO Routers** Zachary Cutlip
15:00	**Sploitego – Maltego's (Local) Partner in Crime** Nadeem Douba	**Hacking the GoogleTV** Amir 'zenofex' Etemadieh, CJ Heres, Dan Rosenberg, Tom Dwenger	**Owned in 60 Seconds: From Network Guest to Windows Domain Admin** Zack Fasel	**bbqSQL – Blind SQLi Exploitation** Ben Toews, Scott Behrens
16:00	**How to Hack All the Transport Networks of a Country** Alberto Garcia Illera	**The Paparazzi Platform Flexible, Open-Source, UAS Software and Hardware** esden, dotAero, misterj, cifo	**Subterfuge: The Automated Man-in-the-Middle Attack Framework** Matthew Toussain, Christopher M. Shields	**SQL Reinjector – Automated Exfiltrated Data Identification** Jason A. Novak, Andrea London
17:30	**Closing Ceremonies In Track 1**			

THANK YOU!

DEF CON is run by volunteers and without them nothing would happen. I want to thank all of the people, teams, and unsung heroes who made this year possible:

Neil, Nikita, Sleestak, Charel, Zac, Nico, Paralax, Moon Shadow, Jeff McN, Dead Addict, LOsTB0Y, Will, Uncle Ira, ETA, Black Beetle, B.C. Cotman, Chris Eagle, Converge for watching over the DEF CON Groups for these past years, and to Blak Dayz for following in his footsteps.

The contests and events team run by Pyr0 and his awesome staff: Mar, TheDon, DenHac, and the 303 DC Planning Committee for their party planning, badge design, and helping those "other kids" win Vegas year after year.

The Vendor Goons: Roamer, AlxRogan, Evil, Latenite, Redbeard and Wad. The Goon Band: Godminus1, Rich, Redbeard, and Deviant. Brennan for doing such a great job on the Vendor Application this year. Wiseacre for his help with the floor plan. All of the DEF CON 20 Vendors.

The NOC staff who keep things running every year: Lockheed, Heather, Mac, effffn, Rukbat, Videoman, Enki, Mac, #Sparky, and t3ase. This year they have interns – Jared, Justin, and Erik!

Speaker Operations staff for all the long hours, sore feet, and missed talks: AgentX: A55mnky, Bitmonk, Bushy, Code24, Crash, Dallas, Dapper Dan, Froggy, Gattaca, Goekesmi, Jinx, Jur1st, KK, Nevada Raven, notkevin, Number2, Pardus, Pasties, Pwcrack, Rich, roundRiver, Shadow, Vaedron, WhiskyRomeo & zendog. Finally to Quagmire Joe, where ever you are, I look forward to the boat drinks.

Thanks to the Production & Dispatch team: Charel, Doolittle, Kampf, Betsy, Mari, Morgan, Rf, Voltage Spike, Chuck, Noise, Ash for leading the Dispatch & Production crew forward.

Thanks to Uncle Ira, and the Logistics Team of Major Malfunction, ETA, RijilV, Alien, Dodger, and Merlin.

The schwag team: SunSh1ne, secret, veruus, Amazon, Atucom, Cpt Fury, dern, diami03, GateKeeper, Gingerjet, globus, g-ziggy, l0rn4, Lisa, owaspgirl, Rudy, and scout.

Information Booth: Ed, Flower, Melloman, Zookeeper, Littlebruzer, Littleroo, Jerel, Fran, Jenn, Sanchez, Sl33pE, algorythm, Leila T., Mojostico, ACR0NYM, Project Chatter, madstringer, Titan. Awesome Folks!!!

Registration team: TW, Tyler, Cstone, Crackerjack, Queen, 6Q, Matt, Aaron, Zane and Melissa!

Security team: b0n3z Blakdayz Captain chosen1 chs cjunky converge cyber dc0de flea Fox gadsden h3adrush HattoriHanzo jake23 jdoll JustaBill kallahar kevine krassi lei Londo Lordy lunaslide mattrix MAXIMUS montell noid nynex P33v3 Pappy Pescador pfriedma polishdave priest quiet rik skydog Synn tacitus trinity Vidiot wham WhiteB0rd Xtasy Evil Phreck Queeg Amber Angie Kruger GM1 Danozano CyMike Fox. Capt Arclight

Entertainment Staff and acts: object D, An Hobbes, Dr. Raid, YTCracker, Dual Core, Dale Chase, MC Frontalot, Mochipet, Saint VII, The Goon Band, Minibosses, REGENERATOR, Cy Fi, Krisz Klink, SailorGloom, phreakocious, Rene, Ryan Gatesman, Electric, Sigma Star, DJ%27, Robb Wise & thad Timothy, Zebbler Encanti Experience, Great Scott, The Crystal Method, Elite Force, Miss DJ Jackalope, Mitch Mitchem, Project Mayhem, Zack Fasel, Keith Myers, VJ Q. Alba, Alba T. Ross, kampf, NOP !

Grifter, Bluknight and Banshee for all the help with the Skytalks

Stealth and his team for the EFF fundraiser shooting contest

ASTcell and Hackerphotos.com thanks for the pics!

Groups like the all the DEF CON Groups worldwide, 303, SecurityTribe, Hektik, 23.org, Phenoelit, Ninjas, DDTEK, Vegas 2.0, EFF

Thanks to Jason Scott and his team for their hard work on the DEF CON Documentary, both pre-con and during the conference. In addition, thanks to all the attendees and staff that took time from their busy schedules to participate. Thanks to Jericho/Dis for his help on the DC Recognize Awards.

I would all like to thank those who have taken their time and money to take a risk and run a contest, organize a hacking village, submit a talk, or perform music, and last but not least the attendees for showing up for 20 years.

Special remembrance to all the brothers and sisters who cannot be with us this year. The good memories and the knowledge you gave us will live on within us all and be shared with many, you will continue to be missed.

-The Dark Tangent