
DEFCON
18

WELCOME TO DEFCON 18.1-ish

Welcome to DEF CON 18, the barely legal edition! There are lots of things happening this year, and not enough room to mention it all. The forum.defcon.org server, despite being a continued target of the pushdo botnet, has been super busy with party and event planning. The site is about as updated as we can make it, but stuff always happens last minute. Follow #defcon on twitter as well as on foursquare to get a handle about what is going on!

I swear the contests exploded this year! I have been meaning to do a tamper evident contest for years, and I finally got around to ordering all the stuff and writing it up this year. I go to post about it in the forums and pow! There are at least twice as many contests this year as last. There are so many ways to get involved and meet new people at DEF CON this year!

Another change is the network. I splurged and bought us a 75Meg symmetrical net connection. Lockheed and the networking team have enabled WPA2 encryption. Now you can get on-line, stream audio or video, share pics from your phone, or whatever. No more waiting for the saturated 3G networks. Just don't hammer us with bit torrent please!

Burned out from all the speaking and contests? Check out the chill out area to grab a drink or just kick back and compute to some chill music. Same place as last year, just with a 2.0 upgrade. Awesome work by the people that brought you the Cartoon Networks Boston bomb scare. Cyborg Dragon Attack!

Yes, the floor plan changed, it is something new to try and better deal with room change crowding. IT let's us put (almost all) the social stuff on one end, and all the speaking content in the other with a wider hallway.

The badges? Yes, I am so confident they are here by now I'll pretend that they are. Check out their metal eliteness! Not only is the badge using some cutting edge tech this year, it is also the hub of several contests and is more hackable than ever. If you happen to also possess a Ninja Networks badge you might find out they play nice together. 'Nuff said.

So as we kick this awesome party off I just want to thank everyone for showing up, contributing the community, and encourage you to get involved. Send all your post DEF CON pics, vids, and stories and we'll get 'em on-line!

— The Dark Tangent

CONTENTS!

NETWORK!

DEF CON NETWORKING!

WIFI
802.11b/g – DefCon
802.11a – DefConA

New this year: DefCon-SECURE

3G got ya down? Just want to get onto the Internet without fear of those pesky hackers looking through your packets? We've setup DefCon-SECURE for you! It's WPA2 secured OTA and trunked direct to the firewall and out to the Internet (after that, you're on your own!). Details for getting your WPA2 creds will be at registration.

Last year we blew out the 20Mbps we had (QikVideos, iPhone OS updates) – so this year The Dark Tangent signed us up to 75Mbps of pure, unadulterated bandwidth! What are we going to do with it all? I'm sure you'll help us figure that out!

Shouts-out to the NOC staff who keep things running every year: Lockheed, Heather, Videoman, efffn, Enki, Mac, Sparky, KidKaos – and this year, introducing DJ t3ase helping us out with web-work and running around.

Let us know how the network's working for you - noc@defconnetworking.org.

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

DEF CON TV!

The Hacker Confessional!

Yes, it's back – the Hacker Confessional. Look for the beautiful grey box and green button near the Info Booth in the contest area. If you're a first-timer, or missed it last year, the Hacker Confessional gives you a chance to make a 30 second video that could make it up on DefCon TV. Last year we watched eta slowly eat his doughnut. What will he do this year? Watch DCTV. defcon.org to find out!

MOBILE MADNESS

Need to know what's happening NOW, and quickly? Want to keep in touch with what track your buddies are going? This year we put together a web-based agenda called the DefCon Moible Edition (DC-ME). It's formatted for use on your mobile phone

HTTP://ME.DEFCON.ORG

It will tell you what's going on at DefCon right now - talks, events, contests. We've tested it with iPhone, Android, and others. It's your quick way to see what's going going on NOW!

In addition, you & your friends and log into the system and, much like FourSquare, "check in" to tracks, events, etc. Let your friends know where you're at so you can join up or coordinate who's seeing what talk, or where you're going for food, or simply go off the grid.

IPHONE APP UPDATED!

After years of misplaced, begged, borrowed, and stolen Defcon schedules, a couple of guys (bedpimp and jedi) decided to do something about it. After two weeks of non-stop coding and data wrangling, the unofficial Defcon iPhone app was born. This year, they've teamed up with the dark side (Darth Null) to bring you the improved iPhone app fresh for Defcon 18. **Available now in the app store.**

THE DEF CON 18 BADGE: FIFTH TIME'S THE CHARM.

A lot has happened since DEF CON's first electronic badge five years ago.

The badges have blinked patterns of LEDs, allowed you to create your own custom scrolling text messages, turned off your television, transferred files from a SecureDigital card over infrared, and pulsed to music using Fast Fourier transforms. People have hacked their badge to become a flame thrower, an audio VU meter, a password generator, an amusement park game, an anti-surveillance system, a blue box, and a polygraph, just to name a few. One group even turned my Ode to the DEF CON 15 Badge poem into a rap song.

We've used technologies like capacitive touch sensors, jumbo LEDs, RGB LEDs, MEMs-based microphones, and microcontrollers ranging in size from tiny 6-pin devices to powerful 64-pin behemoths. We've used small coin cell batteries and large camera batteries. We've supported accelerometer and 802.15.4/ZigBee wireless features along with a bunch of hidden and secret modes that most people never took advantage of.

Badge development has happened on airplanes, in shuttle buses, on my honeymoon, in hotel rooms, and while on safari. Badges have arrived with plenty of time before DEF CON and twice they've arrived the first day of DEF CON, much to the chagrin of thousands of people who had to stand in line to exchange their temporary paper badge for the real deal. And, we've run out of badges every time (contrary to popular belief, estimating the number of people who will be coming to DEF CON is not a trivial matter).

The DEF CON 18 Badge is a culmination of prior years' experiences, both good and bad.

The pièce de résistance is a 128-by-32 reflective cholesteric LCD by Kent Displays. This module was originally designed for use in Verbatim InSight USB Portable Hard Drives and has since been made available to other customers. A key feature of the display is that it requires no power to retain the image on the screen, making it ideal for battery-life challenged applications like the badge.

A Freescale MC56F8006 Digital Signal Controller (http://tinyurl.com/mc56f8006-info/) serves yet again as the heart of the unit. For those keeping score, these are the pieces we tried to get through Chinese Customs last year for DEF CON 17 after our original quantity was detained. These were also held, but eventually released to me two months after the conference. Firmware development is done with CodeWarrior for 56800/E Digital Signal Controllers Special Edition (http://tinyurl.com/mc56f8006-dev/ and on the DEF CON CD).

In our quest to create a never-been-done-before artistic element, we laser engraved the DEF CON 18 artwork onto aluminum substrate printed circuit boards, a feat questioned even by e-Teknet, our trusted fabrication and assembly facility. We avoided Customs delays by shipping through Macau, a special administrative region with different rules and regulations than mainland China. We reached out to the DEF CON community to invite people and groups to hide functionality or chunks of data within the badge. We've listened to your comments and provided a USB connection for simple firmware reprogramming via static bootloader, a JTAG footprint for those who accidentally brick their badge during hacking, and a command-based API for controlling the LCD to make it easier for non-hardware people to get involved in badge experimentation.

BADGES

My Making the DEF CON 18 Badge presentation covers the entire design and development process of the badge, along with details of badge functionality. All engineering documentation, including schematics and source code, is available on the DEF CON CD and my web site (http://www.grandideastudio.com/portfolio/defcon-18-badge/)

Whether this is your first time at DEF CON or you're a seasoned regular, I strongly encourage you to poke around and see what your badge can do. Modify it, break it, learn something new with it. Participate in the Badge Hacking Contest where the most ingenious, obscure, mischievous, or technologically astounding hacks will win prizes and fame. Use it to teach your friends or your kids about electronics. Design a new product with it. Sell it to someone else. Just don't let it go to waste.

A lot has happened since DEF CON's first electronic badge five years ago.

Within the hacker community, conferences and parties using electronic badges have become the norm. What used to be a unique exception is now the rule. As one who doesn't like to follow trends, I don't know what next year will bring. Just expect the unexpected.

Joe
$KINGPIN$

DEFCON 18 MUSIC

THE ZOMBIE BALL

FRIDAY 8PM-3AM+?

CAPRI 101/102

HIGHSAGE ELECTRONUSERS.COM | TEKFUNK RECORDS

HARBINGER HUMAN LIBERATION FRONT | HLFMUSIC.NET

SAILORGLOOM AGENTS OF EMPIRE DJS | STUTTGART-SCHWARZ

THE WAZTY BOYS NUBREAKS.COM

SUGARPILL DALY CITY RECORDS | GLITCH.FM

GREAT SCOTT MUTI MUSIC | SCARCITY RECORDS

KRISZ KLINK DEFCON | KONTROL FAKTORY

CYBERPUNK GALA

SATURDAY 8PM-3AM+?

CAPRI 101/102

DRRAID SOPHSEC INTRUSION LABS

DUAL CORE DUALCOREMUSIC.COM

ERIC YO! BASSDRIVE.COM | DEEP | HEAVY

PROFESSORPIOUS SMGU | LOST IN BASS | GLITCH.FM

MITCH MITCHEM MENACE TO SOBRIETY | WE GO BANG

MISS JACKALOPE DEFCON | 303

REGENERATOR ALFA-MATRIX.COM | WTFRECORDS.COM

SINEWAVE MUTAGEN RECORDS

THE POOL

FRIDAY 6PM-11PM

MALICIOUS LOGIK SOUNDCLOUD.COM/MALICIOUS-LOGIK

DJ OVERZERO DJOVERZERO.COM

FILLMATIC SWAY NIGHTCLUB SAN DIEGO | DJFILLMATIC.COM

DJ LAHBUG HELIX SF | EVENTBRITE | GOOGLE

ALEX M DJMIX.NET | PROGHOUSE.COM | PROTON RADIO

THE POOL

SATURDAY 6PM-11PM

SIMPILL MAMBO RECORDS | THE SOULSCAPE COLLECTIVE

RYAN GATESMAN SUB ASSASSINS | DIRTY FABRIC

TWINKDOGG NUBREAKS.COM | WARRIOR BREAKS

AFRO MONK MIAMI GLITCH | GLITCH.FM | AFROMONK.COM

CHRIS B PORTAL PATCH | SOUNDCLOUD.COM/CHRISBMUSIK

SOUND: MOBIUS
MOBIUSPROAUDIO.COM

VJ: PSYBORG, SPOOKY NOODLE GHOST, SHAMI, SHADOWVEX, VJ Z3X, ZEBBLER
2132104444 PSYTRIP.TV SHADOWVEX.COM

DECO ART: KATE VAN REES + ZEBBLER
ZEBBLER.COM

CONTESTS!

10,000¢ HACKER PYRAMID,

Saturday 21:00 to 22:00. in Speaking Track 4

The 10,000¢ Hacker Pyramid is a classic game show take off with the kind of pizazz that only teams composed of average DEF CON Attendees and (in)famous DEF CON Celebrities could possibly bring to the stage. In a series of rounds, 8 teams will vie for the ultimate prize - 10,000 Canadian Pennies! Watch as Dick Clark's worst nightmares come true and a new DEF CON tradition is born. And don't feel bad for the losers - we've got prizes for them too - AWESOME prizes.

50,000 "CRACK ME IF YOU CAN" PASSWORD CRACKING CHALLENGE

On Friday - at a specified time, KoreLogic will release a file containing 50,000 encrypted passwords. These passwords will be of varying types (such as SHA, SSHA, DES, Lanman, NTLM) and will range from being "easy" to crack - to extremely difficult to crack. The goal of the contest is two-fold:

1) To crack as many passwords as possible

2) To crack all the "administrative/root" passwords.

Prize of $1,000 will be offered.

BADGE HACKING CONTEST

All Con until Sunday

The DEF CON Badge Hacking Contest awards the top 3 most ingenious, obscure, mischievous, obscene, or technologically astounding badge modifications created over the weekend.

BACKDOOR-HIDING CONTEST

Friday-Sunday Contest Area

The CoreTex Competitions Team from Core Security is happy to announce the 1st Open Backdoor Hiding & Finding Contest to be held at DEF CON 0x12 this year!

Hiding a backdoor in open source code that will be subjected to the scrutiny of security auditors by the hundredths may not be an easy task. Positively and unequivocally identifying a cleverly hidden backdoor may be extremely difficult as well. But doing both things at DEF CON 0x12 could be a lot of fun!

BEVERAGE COOLING CONTRAPTION CONTEST

Friday 12:00 to 14:00

If there's two things that many hackers know, it's how to enjoy a frosty, refreshing beverage and how to leverage technology to make life better... or at the very least, more entertaining. The Beverage Cooling Contraption Contest asks the question: if you were to be stranded in a hot, dry climate... would you be able to take cans of liquid refreshment sitting at room temperature and turn them into something more palatable?

CAPTURE THE FLAG

Friday-Sunday in the CTF Room.

DEF CON Capture the Flag, the premier annual hacking throw down that pits teams of ninjas against each other in a multi day battle for pwning supremacy. Each team defends multiple services while attempting to own services defended by other teams.

CAPTURE THE PACKET

Friday & Saturday in the Contest Area

Contestants will attempt to solve a number of challenges varying in difficulty within the "Capture The Packet" network traffic. Clues describing how to complete each challenge will be contained within the traffic. Contest consists of a preliminary round and a final round. Prizes to be given for the 1st-3rd place winners.

CRASH AND COMPILE

Saturday 20:00 to 01:00 in the Contest Area

Crash And Compile: An ACM style programming contest turned into a drinking game. Code doesn't compile? Take a drink. Code doesn't produce the right output? Take a drink. Wackiness ensues. What could /possibly/ go wrong?

DARK TANGENT'S TAMPER EVIDENT CONTEST

Friday-Sunday in the Contest Area

You will be given a package. This package will have tamper evident seals on it. Some of these products claim to be "Impossible to reseal or reuse". Your goal is to prove them wrong and document your work every step of the way.

CONTESTS

GRINGO WARRIOR

Saturday 14:00-18:00 in the Contest Area

What happens when a good time goes bad? Imagine you are traveling south of the border and are kidnapped by criminals intent on extortion. Could you use your wits, stealth, and a hidden set of lockpicks to escape to freedom? Like last year at DEF CON, the main lockpicking competition will be a scenario-based game in which contestants must use picking skills to free themselves from evil captors in under five minutes. The course will offer a variety of locks representing a range of difficulty, allowing participation by people of all skill levels. Points will be awarded based on the time of completion as well as the difficulty of locks attempted. Big fun for all involved and super-kickass prizes for the winners.... come and have fun being a Gringo Warrior!

HACKER JEOPARDY

Friday & Saturday Track 1, 21:00 to ??

Hacker Jeopardy is Def Con's, biggest, first and longest running game … and we're back again! Oh yeah!

Join 2,500+ of your fellow DefConners to watch contestants be humiliated, drink, answer really tough geeky questions, drink, sell their clothing for points, drink, and try to calculate long Hex, ASCII and Port Math questions while drinking. It starts, as usual, at 9PM on Friday night for two games where the teams (of up to three people each) fight it out, duke it out and drink it out with questions to our answers. 9PM on Saturday brings Round 3 and the Final between the first three games' winners. Winners get awesome stuff from DT… like Black Badges! And more. Losers get to drink. Audience Drinks. All players drink. (>21 Only)

Hacker Jeopardy is rated Heavy-R. You are warned – but we have to be somewhat cool in the Riv cause it's a casino hotel.

LOST @ DEF CON MYSTERY CHALLENGE

brought to you by Ryan "LosT" Clarke

DEF CON 18 marks the fifth year for the Mystery Challenge. Repeatedly I'm asked just what exactly the Mystery Challenge is. The only answer that seems to fit is, "It's the Mystery Challenge". Now before we get into a discussion on circular reasoning, I'll try to sum it up the best I can. The Mystery Challenge is a hacker game meant to touch all aspects of hacker culture. In the past this has included crypto, circuit building, mathematics, social engineering, linguistics, hardware hacking, riddle solving, and many other areas of interest to those with a hacker mindset. Teams attempt to solve puzzles and questions, without foreknowledge of what their objective even is. The most difficult part of the contest is being able to pick signal out of noise. I hope that the entire journey is enjoyable. Mystery Challenge Homepages: Ten-Five-Seven.org, LostboY.net

NETWORK FORENSICS PUZZLE CONTEST

Friday 13:00 to Sat 10:00 in the Contest Area

Ann Dercover is on the run, and you're hot on her trail as she travels around the globe hacking companies, stealing intellectual property, launching 0-day attacks and setting up sneaky backdoors. *You are the forensic investigator.* You've got a packet capture of Ann's network traffic. Can you analyze Ann's malicious traffic and solve the crime by Sunday? Prize: Win a brand-spanking new Apple iPad!

OCTF

Friday-Sunday in the Contest Area.

Open Capture the Flag (oCTF) is a computer security wargame open to all attendees of DEF CON. All individuals are permitted to play given physical/network room and that they follow the rules as designated by The Tube Warriors. The contest will focus on binary exploitation, reverse engineering, forensics, web security, networking, etc. Teams will be pitted against each other to take control of services and gain points by holding onto control of them.

REVOLUTION SECURITY CONTEST HACK

Pentest on new and completely Revolutionary Technology that provides transaction level encryption, every packet has a new independent unique key mutually authenticating both ends of the conversation.

TWITTER HUNT

"Each day at DEF CON you will have an opportunity to blag yourself a sweet limited edition DEF CON-ized skateboard deck. There may also be a couple of signed Tony Hawk decks slung in for good measure too... who knows. You will have to follow @TheSuggmeister (http://twitter.com/TheSuggmeister) during DEF CON to know where to look. He'll be tweeting clues which lead to prizes. Hashtag #DefconTH"

SPOT THE FED

Every year this contest doesn't change. You think someone is a FED, you tell a goon. If you are right you win. If you are a FED and you are spotted, congrats, you're obvious and you win a T-shirt. You know you want the t-shirt.

Official DEF CON Swag

08:00 - 22:00

Thursday and Friday at the West Reg Desk.

Saturday & Sunday at J!NX in the Vendor Area.

BOOK SIGNINGS AT BREAKPOINT BOOKS IN THE VENDOR AREA

JAYSON E. STREET

Author of "Dissecting the Hack: The F0rb1dd3n Network (Revised Edition)" by Jayson E. Street, Kent Nabors & Brian Baskin

ISBN: 9781597495684

Book Signing Friday at 13:00

CAMERON MALIN & JAMES AQUILINA

Authors of "Malware Forensics"

Book Signing Friday at 14:00

DEVIANT OLLAM

Author of "Practical Lock Picking"

ISBN: 9781597496117

Book Signing Friday at 15:00

RICHARD THIEME

Author of "Mind Games"

Book Signing Saturday at 14:00

EVENTS!

THE ART OF YETI

Friday - Sunday in the Contest Area

Be sure and come by and see the psychotic art of Eddie Mize in the contest area. You will remember it from last year if you went through the contest area at all or if you saw Kingpin's Uber Badge or any of the other hundreds of badges Eddie drew on. Eddie is donating a significant portion of the proceeds to EFF again. Last year (with your help) he raised over $1,200 for EFF. Eddie will be drawing on badges again this year for a donation to EFF as well.

DEF CON MASSAGE TABLE

Friday - Sunday in the Contest Area

Artful Touch Massage of Seattle, in association with Serenity Massage of Los Angeles, will be offering massage services in the contest area of DEF CON this year. The cost is $20 for 15 minutes, first come first served. The two licensed Practitioners, Courtnee and Jessica will be offering rejuvenating, mainly oil-free Thai, Sport, and Chair Massage. When you want to take a breather or get your neck funk worked out, you can do so without a lot of fuss or cost. Learn more about them at their websites: http://artfultouch.info & http://www.serenitymassageonline.com

FORUM MEET

Friday 21:00 - 02:00 in Skybox 205

Come hang out at the forum meet! Meet the people of the DEF CON Forums. Listen to the wisdom of the ages, meet new people like yourself, learn a little or a lot. Join the mysterious community that hangs out online the rest of year between shows!

21:00 - 22:00 Official Meet and Greet.
22:00 - 23:00 Special Guests, Door prize giveaways, DEF CON Trivia game.
23:00 - 02:00 Party Lounge

A special prize will be awarded to one lucky forum member during Sunday's award ceremonies! Show up to the forum meet to enter!

GOON BAND

Friday 20:00 in the Contest Area

The Goon Band returns for their second year with even more musical mayhem. Join us Friday night, at 8pm, in the Contest area for the best way to get the evening's parties started. The mosh pit was great last year, but we'd like to triple the size this year. Just be sure to take off your badge, first! The Goon Band is Roamer, y3t1, GM1, vertig0, and Doc.

HACKER KARAOKE

Thursday and Saturday 21:00 to 02:00 in Skybox 212

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". Follow us on Twitter: @hackerkaraoke

HACKERS & GUNS IN LAS VEGAS

Friday-Sunday in Capri Room 103.

Fire Arms Training System to benefit the EFF.

MOHAWKS FOR EFF

Friday-Sunday in the Contest Area. Times Posted.

"I'm going to force people to give money to the EFF by holding them down and shaving the sides of their heads."
- Ed Word

PODCASTER'S MEETUP

Friday in Speaking Track 2 21:00 to 22:00

The Podcaster's Meetup is a LIVE broadcast podcast that includes a panel of all the security podcasters present. Its an event for listeners to meet podcasters and podcasters to meetup with their listeners. Bloggers, coders, hackers, geeks, everyone is welcome to the event, and if you want to be on the show, that just might happen as well.

QUEERCON

Fri: Mixer 16:00 in DJ/Chillout, 22:00 in Skybox 210

Queercon is BACK! For the seventh year in a row, bigger and better, we're out and having more fun than you can shake a glowstick at.

Looking for a place where you can relax, cut loose, and meet people like yourself? Both Friday and Saturday afternoon at 4PM, join us for a laid-back prefunk in the DJ Chillout area (101/102). Come drink, socialize, and swap stories.

Friday night starting at 10PM in Skybox 210, we'll turn up the bass for the hottest dance party EVAR! We have an amazing space, international headliner DJs, and a top-notch system to keep the music going all night long. Best of all, it's FREE and everyone is welcome. Hope to see you there!

THE SUMMIT

Thursday, 20:00- 04:00, Monaco Tower - Penthouse "Top of the Riv"

Vegas 2.0 once again proudly presents "theSummit 6"! theSummit is a Fund Raiser for the Electronic Frontier Foundation on Thursday Night between Black Hat and DEF CON events. It features Black Hat, DEF CON and Security Speakers from across the globe. They all come into this small venue to talk directly to YOU. That's right! Want to pick Joe Grand's brain about the badges? Maybe you want to get some secrets for LoST's Mystery Box Contest? Or perhaps you just want to have a beer and talk shop with Winn Schwartau. Any way you cut it, you get direct access to some of the current thought leaders in the Security Industry AND get to support a great cause, the EFF! We have expanded the space to accommodate 450 people Plus Stage for DualCore, MiniBosses and DJ Jackalope.

$40 at the Door

**Each entry comes with a 1 year membership to the EFF and one raffle ticket. **Cash only. **Additional donations to the EFF will be accepted.

Follow Us on Twitter for Event and Feature Guest Updates: @effsummit

TOXIC BBQ

17:30 - 21:00 Thursday, Sunset Park, Picnic Spot: AREA F

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.

http://www.toxicbbq.com/

WALL OF SHEEP

Friday-Sunday in the Contest Area

The Wall of Sheep is an interactive demonstration of what can happen when users let their guard down. We passively observe various traffic, looking for weaknesses in applications and protocols including users logging into email, web sites, RFID, or other system without the protection of encryption. Those we find get put on the Wall of Sheep as a good-natured reminder that a malicious person could do the same thing we did . . . with far less friendly consequences. More importantly, we strive to educate the "sheep" we catch – and anyone who wants to learn – how to use free, easy-to-use tools to prevent leaks in the future * Gawk - At the "Sheep" caught logging in insecurely

* Hope - That it's your Boss/coworker/archnemesis on the Wall and not you

* Learn - How to protect yourself and how to catch "Sheep"

* Test - your sheep-catching techniques.

EVENTS

HANDS-ON!

HARDWARE HACKING VILLAGE

Friday-Saturday 10:00 - 19:00
Sunday 10:00 - 15:00

This year the Hardware Hacking Village is attempting to reach out to those who have not yet ventured into electronics hardware. Kits for sale in the vendor area will be supported with classes (possibly on demand) helping people get through the initial 'set-up' hurdles that often prevent people from branching out into this arena. Although the village is open to everyone, we understand that it can be intimidating for those new to electronics to get started. So come join us. Learn to turn on LEDs. Learn to control servos. We're here to help. Hopefully you can go home from this year's DEF CON with enough knowledge that armed with Google and other references you can continue on your journey to becoming a hardware hacker.

LOCK PICKING VILLAGE

Fri-Sun in Skybox 211/212

Want to tinker with locks and tools the likes of which you've only seen in movies featuring cat burglars, espionage agents, or Southern California car thieves? Then come on by the Lockpick Village, where you will have the opportunity to learn hands-on how physical security hardware operates and how it can be compromised.

The Lockpick Village is a demonstration and participation area on the skybox level at DEFCON. In this workshop environment attendees can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice with locks of various levels of difficultly to try such tactics themselves.

Experts will be on hand to give demonstrations, 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. After all, you can have the most hardened, patched, and properly-configured servers on the planet but none of that matters if someone marches them out the door without any difficulty.

DEF CON 101

Thursday, Track 1
13:00 - 15:00

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.

This year, some DEF CON veterans will give a glimpse into their own journey and speak about how they got involved with the Community. You'll hear from the man himself (DT), talk about ... well, whatever he wants to talk about. (After all, it is his party.) Pyr0 will give an overview of the contests and games this year (and there are a lot of new ones!). HighWiz will wrap up the first hour with a DEF CON Survival Talk.

After a ten minute intermission we'll be right back...

DEF CON 101 is Sponsored by Runnerup, HighWiz and the letters F, A, and G.

We'll be trying something new this year with the inclusion of three mini-games that we hope will give your the opportunity to actually participate on a new level with some of the groups involved in DEF CON.

Lost and his Mystery Challenge will be running one mini-game while Siviak and the Scavenger Hunt Pirates run another. The third "World Domination" is sponsored by gayhackers.org

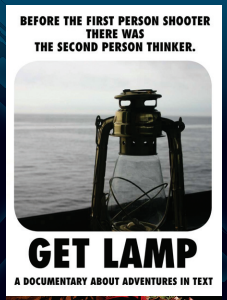
The DEF CON 101 speakers : TheDarkTangent, Lockheed, Jenn, GM1, Pyr0, HighWiz.

Mini-Game Runners : Lost, Siviak, GayHackers

DEF CON 101 Helpers: Xodia and Ripshy

Most of the speakers at DEF CON 101 also believe that using your real name when presenting at DEF CON is kinda lame.

MOVIE NIGHT!



GET LAMP *Thursday in Track 4, Panel at 20:00 Movie at 21:00*
At the dawn of the era of home computing, an unusual type of game was the most popular to play. With just a screen of text and a prompt, you'd be asked the simple question: WHAT DO YOU WANT TO DO NEXT?

As you typed in commands and sentences, the games would tell you a story, a story fraught with danger, excitement, puzzles and hours of exploration. They were called text adventures, adventure games and interactive fiction. They dominated the sales charts and introduced millions to the power and flexibility of home computers. No other type of computer game could come close. And then they were gone forever... or maybe they never actually left.

GET LAMP tells the story from a cave in Kentucky to the modern era of what some call a brand new form of literature. Director Jason Scott will be on hand for the showing, as well as a Q&A afterwards.

ROBOGEISHA *Friday in Track 4 at 21:00*
Think b-grade over the top mash up of robo ninjas, corporate mafia wars, chicks with swards coming out their asses, and a classic love story. From one review by McCormick Kenny "Ah, geisha. Beautiful. Alluring. Mysterious. Robotic. Yoshie is the archetypal younger sister, overshadowed in all ways by her elder sibling. Sis is confident. Yoshie is not. Sis is climbing through the ranks of a local geisha house. Yoshie scrubs the walls and performs menial tasks. Sis is in love with the young head of a local steel outfit. Yoshie ... wait a minute ... Yoshie is the one that he actually prefers! This is a recipe for conflict ... The latest effort from the crew behind cult titles Machine Girl, Sukeban Boy, Tokyo Gore Police and Vampire Girl Versus Frankenstein Girl, you pretty much have to know going in exactly what you're going to get with RoboGeisha - a violent, unrepentantly silly b-film loaded with wildly over the top set pieces hatched from the fevered mind of perpetual adolescent Iguchi."

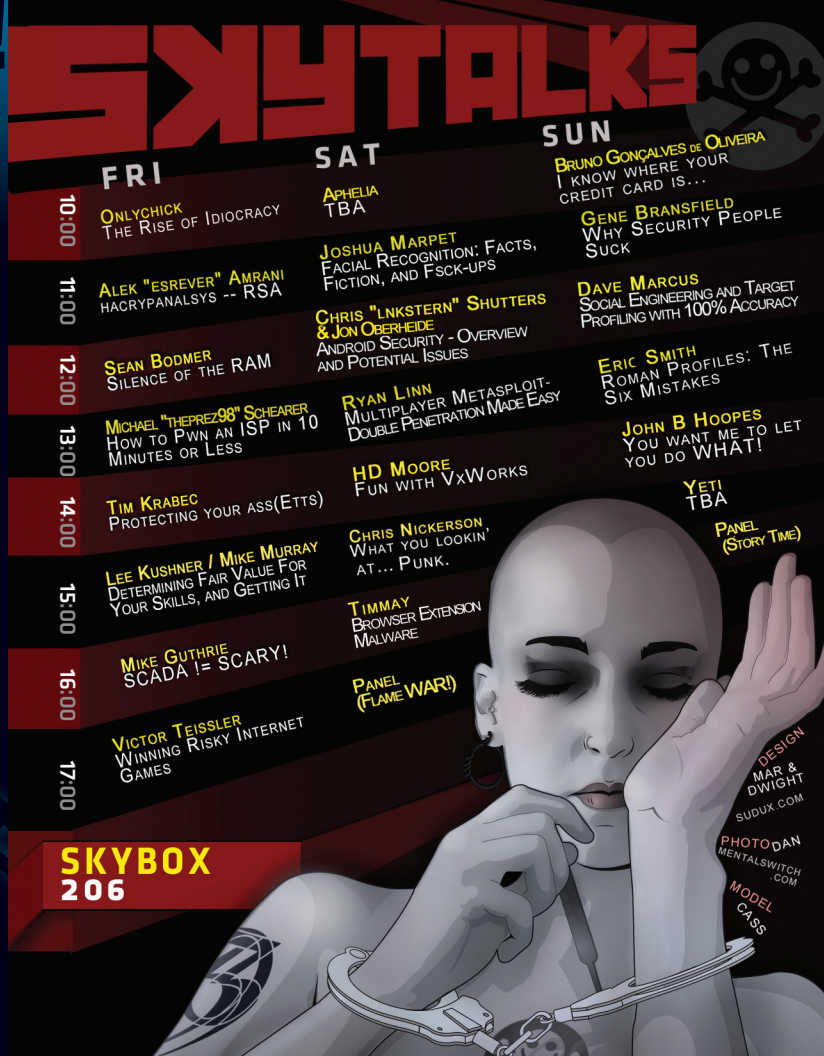
REPO! THE GENETIC OPERA *Saturday in Track 4 at 21:00*
Came out in 2008 and hit cult status soon after. From Wikipedia "American rock opera-musical film directed by Darren Lynn Bousman. The film is based on a play written and composed by Darren Smith and Terrance Zdunich." This sort of reminds me of a Rocky Horror Picture Show in the future where people have gotten loans to replace failed internal organs - and if you fail to make payments Repo men come to repossess them. I've never played a musical, and this isn't my favorite film, but it is unique! To give you an idea of how you either like it or hate it check out some of these reviews also from Wiki:

The film review aggregating website Rotten Tomatoes reports generally negative reviews, with only 33% of reviews being positive. The consensus of the film given is: "Bombastic and intentionally gross, Repo! The Genetic Opera has a unique style, but lacks the wit and substance to be involving." Horror.com called it "a spirited, absorbing, astounding, thought provoking futuristic fulsome fable". Bloody Disgusting website wrote that it was "fresh, unique and exciting... remarkable". This was followed by horror network FEARnet who branded it "an instant cult classic" and "absolutely mind-blowing on a visionary level" according to Canada's Horror-movies.ca.

SKYTALKS

	FRI	SAT	SUN
10:00	Onlychick The Rise of Idiocracy	Aphelia TBA	Bruno Gonçalves de Oliveira I know where your credit card is...
11:00	Alek "esrever" Amrani hacrypanalsys -- RSA	Joshua Marpet Facial Recognition: Facts, Fiction, and Fsck-ups	Gene Bransfield Why Security People Suck
12:00	Sean Bodmer Silence of the RAM	Chris "lnkstern" Shutters & Jon Oberheide Android Security - Overview and Potential Issues	Dave Marcus Social Engineering and Target Profiling with 100% Accuracy
13:00	Michael "theprez98" Schearer How to Pwn an ISP in 10 Minutes or Less	Ryan Linn Multiplayer Metasploit-Double Penetration Made Easy	Eric Smith Roman Profiles: The Six Mistakes
14:00	Tim Krabec Protecting your ass(Etts)	HD Moore Fun with VxWorks	John B Hoopes You want me to let you do WHAT!
15:00	Lee Kushner / Mike Murray Determining Fair Value for Your Skills, and Getting It	Chris Nickerson What you lookin' at... Punk.	Yeti TBA
16:00	Mike Guthrie SCADA != SCARY!	Timmay Browser Extension Malware	Panel (Story Time)
17:00	Victor Teissler Winning Risky Internet Games	Panel (Flame War!)	

SKYBOX
206



SCORING CTF!

SCORING A CTF IS A CHALLENGING PROPOSITION. IN ORDER TO BECOME A MASTER OF BINJITSU, IT IS ESSENTIAL TO UNDERSTAND HOW YOU WILL BE MEASURED.

True binjitsu masters understand that the path to enlightenment may only be achieved by maintaining the delicate balance between the offensive and the defensive arts. This year CTF scoring follows the approach introduced last year for measuring what is happening in the game and is designed to reward offensive as well as defensive excellence. 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).

Rather than simply awarding a point per stolen or overwritten 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.

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.

Item 5 above is meant to ensure that a team does not simply shut down all of its services in order to achieve a perfect defense (and make a boring game for everyone else).

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.

In the CTF room each team is assigned a unique color which is reflected by their team banner, tablecloth and on the scoring displays. The contest allows each team to have at most eight players at the table at any time (though some teams likely have additional resources beyond what is visible at the table). Teams are allowed to bring in whatever tools they prefer.

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

CHECK OUT ALL THE WAYS YOU CAN KEEP UP WITH DEF CON BEFORE, DURING AND AFTER THE SHOW!

Join the forums for discussions, news and planning of next years DEF CON!
https://forum.defcon.org

Upload all your Photos and share your DEF CON memories at
https://pics.defcon.org

Direct from the tubes, get your DEF CON News on the DEF CON RSS Feed
defcon.org/defconrss.xml

Check out Twitter for the freshest DEF CON updates!
twitter.com/_defcon_

Our Facebook page has news, photos, videos and special content!
facebook.com/defcon

Get in touch with other Hacker professionals in our LinkedIn group!

VENDORS!

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.)

lbgfx.com Customize T shirts & Stickers on the spot at DEF CON 18

University of Advancing Technology (UAT) The University of Advancing Technology (UAT), in Tempe, AZ, is a private university for geeks that merges the values of the traditional academy with the modern technology campus. UAT creates a distinct, non-exclusionary and geek-friendly university in which students learn to value their own uniqueness and the power of technology in education. UAT is home to over 1200 on-campus and online students and faculty members, and offers 20 undergraduate degrees and five master degrees. Our year-round balanced learning methodology represents an evolution of established educational methodologies with possibilities afforded by technology in that it foresees an evolution of student learning techniques and tools, and is designed to improve knowledge retention and lifelong learning.

simpleWiFi Alfa and AirWaveData high power USB adapters, Access Points (AP), Outdoor AP and CPE Ethernet units, Long Range Booster antennas including Yagi Cantenna, Parabolic grid, Patch, dipole, rubber flex, omni-directional and marine types. LMR-400 and other cables plus all kind of connectors.
9500 NW 12 ST #4 Doral, FL 33172 305-798-8505

DIFRwear Our mission is to give individuals the ability to maintain privacy and ensure security in a world of insecure contactless devices. To fulfill this mission, we realize that individuals require devices that supersede the default, and often inadequate methods of securing RFID tags. We produce stylish clothing and accessories that block RFID technologies.

HotWAN HotWAN strives to provide the Hacking and Security Communities the best of Penetration Test Gear. We focus on combining hardware, open source and commercial software in building cross-platform attack systems ideally suited for the mobile user. Optimized and versatile, these systems keep the user on the bleeding edge of today's toolsets across multiple operating systems as well as provide the necessary support documentation in the latest hacking techniques.

Irvine Underground Organization IrvineUnderground.org is a group of people located in and around Irvine, California [www.liveirvine.com] and the major Orange County area. June 2002 marked the group's first meeting which only five attendees showed up for; since the launch date the word has spread bringing in a much larger crowd.

hackerstickers.com

Lock Picking 101

no starch press No Starch Press publishes the finest in geek entertainment — distinctive books on computing, such as bestsellers Steal This Computer Book, Hacking: The Art of Exploitation, Practical Packet Analysis, and the Manga Guides. We focus on open source/Linux, security, hacking, programming, alternative operating systems, and science and math. Our titles have attitude and our authors are passionate.

Ghetto Geeks We welcome everyone to this year's DEF CON. We have been around providing clothing for the community for about 10 years now, and we're still at it We enjoy seeing friends both new and old we look forward to showing you exactly why Ghettogeeks is still around: you. Come by and sign up on our promotions list, and we'll even give you a sticker. As always, let's get down and enjoy what we do best: hacking.

GUNNAR OPTIKS GUNNAR Optiks is a revolutionary technology that has been adopted by hundreds of doctors (and counting) as a primary computer vision solution for patients suffering from symptoms of CVS (Computer Vision Syndrome), as well as a growing in-office or in-class necessity, and a "must-have" accessory for gaming. GUNNAR is VSP approved and also covered by Vision Care Direct Vision Plans.
For more information, please visit our website: www.gunnars.com/technology

HNN Editor in Chief and News Anchor, Space Rogue, founded the Hacker News Network as a "blog before there were blogs" in 1998. For over two years, Hacker News Network was the "Voice of Reason" (a phrase given to it by MSNBC) for computer underground and Internet security related news stories. While HNN has been on a ten year hiatus the Snake Oil, FUD and other shenanigans in the computer security industry never went away and the dumbed down level of reporting in the mainstream media still exists and is worse than ever. Space Rogue and Tan have resurrected The Hacker News Network and have returned with HNNCast, The Buffer Overflow, Behind the Firewall, and other shows to be announced soon. This effort will attempt to expose, educate and spread the truth, not only about security but the news that involves the people of this community. The Hacker News Network and HNNCast have been redesigned to fit a new era in Internet based news broadcasting.

Surplus "Home of the $99 1U Server"
1260 La Avenida St
Mountain View, CA 94043
Toll Free: 877-UNIX-123 (877-864-9123)

EFF The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. EFF believes protecting innovation is central to advancing our freedom and has fought to clear the way for open source software, encryption, VoIP, file sharing tools, and much more. We defend free speech on the Internet, fight illegal surveillance, promote the rights of innovators to develop digital technologies, and work to ensure that the rights and freedoms we enjoy are enhanced, rather than eroded, as our use of technology grows.

MECO Moser Electronics Company Your source for workstations and networking equipment and then some…
PO Box 939
Snohomish, WA 98291-0939
Tel: (425)788-0208 Fax: (360)794-8754
Serving the Industry since 1980

Security Snobs.com SecuritySnobs.com sells high security mechanical locks including door locks, padlocks, cutaways, collector locks and more. Security Snobs sells the highest security products including from top manufacturers like Abloy, BilLock and offers a wide range of other high security products.

breakpoint Books & More 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!

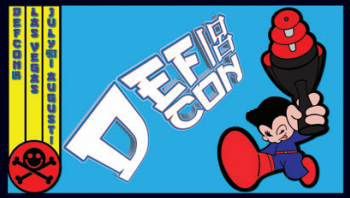
Greensector: Stop by our booth for unique limited-run t-shirts designs, DJ mixes, stickers, buttons, post cards & other nick-hacks. Presented this year in 3D!

J!NX J!NX has been a fixture in the vendor area of DEF CON for 11 years, providing hackers with enough tees to avoid doing laundry. Check in at the booth for regular giveaways and a few special surprises!

ART CONTEST!

CONGRATULATIONS TO THE DEF CON 18 ARTWORK CONTEST WINNERS!

"18 & Legal" by Mar – 1st Place and Peoples Choice



"DEF CON Boy" by oshu – 2nd Place

"Her" by emtag – 3rd Place

DC-949 PRESENTS CATROULETTE

Chatroulette with Netcat. Catroulette, or Catr for short, is an experimental communications service in which willing participants connect to a server on a specified port with Netcat, Telnet, etc. and are randomly connected with another user who has done the same. Connect, meet new people, make arrangements for contests, food runs, bar hopping, whatever. Simple? sure. Convoluted? Yep. Fun? guess we'll find out! Connect to the local server on port 9000, available from anywhere on the DefCon network, with the dns entry "catroulette" example: netcat -v catroulette 9000

PRESENTATIONS

FOCA2: THE FOCA STRIKES BACK

Chema Alonso *MS MVP Enterprise Security. Informatica64*
Jose Palazon "Palako" *Security Researcher*

FOCA is a tool to extract information in footprinting and fingerprinting phases during a penetration test. It helps auditors to extract and analyze information from metadata, hidden info and lost data in published files. This new release of FOCA, version 2, adds tools to scans internal domains using PTR Scanning, Software recognition through installation paths, etc. The idea of FOCA is to give as much info as can be discovered automatically starting from a public domain name.

CONNECTION STRING PARAMETER ATTACKS

Chema Alonso *MS MVP Enterprise Security. Informatica64*
Jose Palazon "Palako" *Security Researcher*

This session is about Parameter Pollution in Connection Strings Attack. Today, a lot of tools and web applications allow users to configure dynamically a connection against a Database server. This session will demonstrate the high risk in doing this insecurely. This session will show how to steal, in Microsoft Internet Information Services, the user account credential, how to get access to this web applications impersonating the connection and taking advance of the web server credentials and how to connect against internal databases servers in the DMZ without credentials. The impact of these techniques are especially dangerous in hosting companies which allow customers to connect against control panels to configure databases.

WPA TOO!

Md Sohail Ahmad *Manager R&D, AirTight Networks*

WPA2 is the most robust security configuration available today for WiFi networks. It is widely used to secure enterprise WLANs. Interestingly, it is also being used to secure guest, municipal and public WiFi networks. In this paper, we present a new vulnerability found in WPA2 protocol which can be exploited by a malicious user to attack and compromise legitimate users. We also present a few attack mitigation techniques which can be used to protect genuine WiFi users.

EVILGRADE, "YOU STILL HAVE PENDING UPGRADES?"

Francisco Amato *Founder, Infobyte Security Research*
Federico Kirschabum *CTO, Infobyte Security Research*

Vulnerabilities are disclosed daily and in the best case new patches are released. Is no new that many application's update process have security weaknesses allowing fake updates injection. The new version of the framework will show how many updates system are still vulnerable to this trivial attack.

CYBER[CRIME I WAR] CHARTING DANGEROUS WATERS

Iftach Ian Amit *Managing Partner, Security & Innovation*

CyberWar has been a controversial topic in the past few years. Some say the mere term is an error. CyberCrime on the other hand has been a major source of concern, as lack of jurisdiction and law enforcement have made it one of organized crime's best sources of income.

In this talk we will explore the uncharted waters between CyberCrime and CyberWarfare, while mapping out the key players (mostly on the state side) and how past events can be linked to the use of syndicated CyberCrime organization when carrying out attacks on the opposition.

We will discuss the connections between standard warfare (kinetic) and how modern campaigns use cybersecurity to its advantage and as an integral part of it.

SCADA AND ICS FOR SECURITY EXPERTS: HOW TO AVOID CYBERDOUCHERY

James Arlen *Security Researcher*

The traditional security industry has somehow decided that they are the white knights who are going to save everyone from the horror of insecure power grids, pipelines, chemical plants, and cookie factories. Suddenly, every consultant is an expert and every product fixes SCADA. And because they don't know what the hell they're talking about — 'fake it till ya make it' doesn't work — they're making all of us look stupid.

Attendees will gain a practical level of knowledge sufficient to keep them from appearing foolish should they choose to opine on any of the various real issues stemming from Industrial Control or SCADA systems. Attendees will also feel embarrassed for something they've said, empowered to call out charlatans, and much less worried about cyberhackers unleashing cyberattacks which cybercause cyberpipelines and cybermanufacturing plants to cybergonuts and cybertakeovertheplanet using cybercookiesofdeath.

EXPLOITATION ON ARM — TECHNIQUE AND BYPASSING DEFENSE MECHANISMS

Itzhak "Zuk" Avraham *Researcher at Samsung Electronics & Partner at PreIncidentAssessment.com*

In this presentation there will be covered (from scratch) quick talk on security mechanisms on X86 and how to bypass them, how exploits are being used on X86 and why they won't work as is on ARM, How to approach ARM assembly from hacker point of view and how to write exploits in the proper way for a remote and local attacker on ARM, what are the options for ARM hacker, etc.

This presentation starts from the very basics of ARM assembly (since there are not lots of expert on this subject) and advance to an expert level of ARM. After this talk you'll think in ARM way.

Today, ARM is running on almost everything (mobile phones, TVs, or tons of other devices). Till now, we were used to think that ARM means no protection mechanisms, which is not the case with the next generation mobile phones.

In the recent/upcoming mobile phones you can start seeing security mechanisms implied. How can you run your shellcode if your stack is not executable? What else do you need to know?

There's almost nothing known on how to exploit weaknesses over ARM in the assembly level, when there are security mechanisms which are very common in X86.

This presentation also presents a technique to create a shellcode which will be able to pass security mechanisms over ARM. For example, this technique can be used to exploit a stack-overflow on ARM when stack is not executable.

WEB SERVICES WE JUST DON'T NEED

Mike "mckt" Bailey *Senior Security Researcher, MAD Security*

A barbecue with a built in webserver. Remote command execution via Twitter. Great geek projects, but do we really need them? On the serious side of things, do we really need web-based management interfaces on firewalls, printers, and phone systems? Maybe it's time to take a look at the sometimes-humorous, often-dangerous downsides.

MOBILE PRIVACY: TOR ON THE IPHONE AND OTHER UNUSUAL DEVICES

Marco Bonetti *Security Consultant at CutAway s.r.l.*

Mobile phones are still a proving ground for keeping the users' privacy safe. This presentation will describe the problems which are arising around the use of these technologies and how they can affect mobile users. It will propose Tor as a possible solution for some of these problems, describing its own strengths and weaknesses and the efforts developers put to implement a working port of the program on different devices, from the Chumby One to my own port for the iPhone platform. Finally, it will also describe where the development is going to protect mobile phone users privacy and let them survive their own devices.

WHO CARES ABOUT IPV6?

Sam Bowne *Instructor, City College San Francisco, Computer Networking and Information Technology Dept.*

What is IPv6? Why should you care? If we ignore it, will it just go away?

The current Internet Protocol numbering scheme, IPv4, is nearing its end-of-life. Within two years, all the IPv4 numbers will be allocated, so that new devices will not be able to connect directly to the Internet. We all will be forced to adapt to the new IPv6 system soon. But how can we get started?

This talk explains why IPv6 is necessary, how it works, and how everyone can quickly and easily start using it now. I will explain and demonstrate how to set up a free tunnel to access the Internet via IPv6.

I will also explain the Hurricane Electric IPv6 certifications. The certifications are great because they guide a novice through the stages of IPv6 knowledge: connecting as a client, setting up an IPv6-enabled Web server, email server, DNS server, and glue records.

There are large security implications to IPv6 too. I will explain several important IPv6 vulnerabilities and countermeasures, including auto-configuration privacy risks, torrents over IPv6, bypassing VPNs with IPv6, Routing Header Zero packet amplification attacks, and the ping-pong IPv6 DoS vulnerability.

My goal is to convince the audience to pay attention to IPv6 and to guide them to an easy way to start learning about it and using it now. All my students at City College San Francisco will have IPv6 homework from now on—you need to get on board now or be left behind!

SECCUBUS — ANALYZING VULNERABILITY ASSESSMENT DATA THE EASY WAY...

Frank Breedijk *Schuberg Philis*

As part of his job as Security Engineer at Schuberg Philis, Frank Breedijk performs regular security scans. The repetitive nature of scanning the same customer infrastructure over and over again made him decide to look for a more automated approach. After building his first scanning scheduler he realized that it actually does not make sense to look at all findings every time they are reported. It would be much better to only investigate the deltas between the scans. The philosophy behind Seccubus was born.

In his presentation Frank will demonstrate Seccubus by performing scans of a live demo environment and explain its inner working and the philosophy behind it.

MASSEXPLOITATION

Michael Brooks *Sitewatch*

This talk covers the use of chaining vulnerabilities in order to bypass layered security systems. This talk will also cover ways of obtaining wormable remote code execution on a modern LAMP platform. These attacks where developed by me, and they are very new. These attacks are as real as it gets, and the results are making the headlines.

"Apocalyptic infection"

— The Register

RESILIENT BOTNET COMMAND AND CONTROL WITH TOR

Dennis Brown *Tenable Network Solutions*

There's nothing worse than toiling away at building a large, powerful botnet after months of effort, only to see it get taken down due to being taken down by an ISP, hosting provider or due to law enforcement intervention. Fortunately, a tool exists that will help us hide the command and control channels of botnets to allow us control our botnets anonymously. This tool is Tor.

This presentation discusses several ways to operate a botnet anonymously via Tor, discuss the strengths and weaknesses of each method, and demonstrate some of these techniques live. Mitigation techniques will also be discussed for all the white hats in attendance.

HOW HACKERS WON THE ZOMBIE APOCALYPSE

Dennis Brown *Tenable Network Solutions*

In April, 2010, a zombie outbreak occurred in Providence, Rhode Island. These were not traditional zombies however; They were controlled by an electronic device that allowed for wireless attacks against the living around them. Fortunately, the living had their own devices, and were able to fight off the zombies... but more threatening enemies entered the fray.

This is the story about the QuahogCon 2010 badge and the embedded Zombie Invasion game. For about 48 hours, hackers attacked not only other players, but the badges themselves, trying to unlock the secrets within. This presentation will explore the various hacks, both hardware and software, that people tried against a system they had little-to-no prior knowledge about, and both the failures and successes that resulted. It will also discuss the decisions made to make the firmware hackable in a way that was accessible to as many people as possible, but not entirely trivial. Further discussion points will cover the hardware used in the badge, some of the more hilarious issues that came up, and will discuss plans for future designs.

EXPLOITING SCADA SYSTEMS

Jeremy Brown *Security Researcher*

SCADA systems are just as vulnerable to attack today than they were ten years ago. The lack of security awareness by SCADA software vendors, combined with the rush of hacking these systems, make them very attractive to hackers today. The focus of this presentation will be showing the disconnect between SCADA software and secure programming. There will be a live demonstration of Sploitware, a framework dedicated to vulnerability analysis of SCADA systems. This framework could be thought of as a proof of concept, although you will see it is more than mature enough to prove the point.

CLOUD COMPUTING, A WEAPON OF MASS DESTRUCTION?

David "VideoMan" M. N. Bryan *Security Consultant & Hacker*
Michael Anderson *Security Consultant, NetSPI*

Using cloud computing to attack systems allows for the testing of a company's incident response and recovery program. We have been using the cloud computing environment to test real world scenarios for different types of attacks, such as Distributed Denial of Service, Flooding, and Packet Fragmentation. The presentation will review some of the common attack types, what they are, and how they can be used to disrupt service. I will also review the steps that led us to choose the cloud computing environment, why these environments are good for most, but also why they may not meet your regulatory requirements. And lastly, I will review mitigation strategies and response programs that can reduce the operational risks when responding to these events.

THE KEYS TO RUNNING A SUCCESSFUL DEF CON GROUP BY DC612

David "VideoMan" M. N. Bryan *Security Consultant & Hacker*
Jared Bird *Security Researcher*

The local DC612 group has been around, and has had a fairly successful attendance for several years now. If you've got a group, or are thinking about running a group we have some pointers for capturing people, and how to keep them coming back for more!

GOOGLE TOOLBAR: THE NARC WITHIN

Jeff Bryner *Owner, p0wnlabs.com*

You downloaded google toolbar because it came with Adobe, or you are a Google fanboy. You started using it to store your bookmarks because you're too lame to rsync them like real man. Little do you know that google is selling you out to your corporate security staff. They now know about the midget porn...the porn you bookmarked at home, but never view at work. Yes *that* porn

OPEN PUBLIC SENSORS AND TREND MONITORING

Daniel Burroughs *Research Associate, University of Central Florida*

Our world is instrumented with countless sensors. While many of these are outside of our control (at least without significant effort...) there is an incredible amount of publicly available information being generated and gathered all the time. While much of this data goes by unnoticed or ignored it contains fascinating insight into the behavior and trends that we see throughout society. The trick is being able to identify and isolate the useful patterns in this data and separate it from all the noise. Sites such as craigslist provide a wealth of wonderfully categorized trend information. What job categories are trending upward? What cities show the most (or the least) promise for technology careers? What relationship is there between the number of bikes for sale and the number of prostitution ads? All of this and more can be explored through data available from this single source – and it is just one of hundreds out there. This exploration was inspired by a past DEF CON talk (Meme Mining for Fun and Profit) and seeks to inspire others to explore the exploitation of such publicly available sensor systems.

BAD MEMORIES

Elie Bursztein *Stanford University*
Baptiste Gourdin *Stanford University Student*
Gustav Rydstedt *Stanford University Student*

No matter which kind of cryptography you are using to defend your network, , sooner or later to make it work you will have to store somewhere a password, a key or a certificate. If the attacker is able to tampers with its storage mechanism then even the strongest encryption mechanism became irrelevant.

In this talk we will present Tapjacking attacks which abuse smartphone features to create more efficient clickjacking attacks. We also show how to attack storage mechanisms to tampers with SSL session and break into Wifi network that use WPA encryption.

For SSL we will show how to exploit warning inconsistency and caching mechanisms to trick the user into accepting a bad cert and gets his credential stolen.

For Wifi network we will demonstrate how to use clickjacking, CSRF, and XSS to steal from routers the two pieces of information that an attacker needs to geo-localize and break into it, namely the WPA key and the mac address. Finally we will discuss how to discuss what frame busting defense are used by the Alexa top 100 website and how we were able to break them using standard and not so standard tricks. We also demonstrate how to use Paul Stone scrolling attack in novel ways.

This is joint work with Dan Boneh and Collin Jackson.

KARTOGRAPH : FINDING A NEEDLE IN A HAYSTACK OR HOW TO APPLY REVERSE ENGINEERING TECHNIQUES TO CHEAT AT VIDEO GAMES

Elie Bursztein *Stanford University*
Jocelyn Lagarenne *Stanford University Student*
Dan Boneh *Cryptography,Stanford University*

While we were slaving away hacking an awesome memory analysis tool, Kartograph, our lazy graduate student friends next door were busy honing their skills in CIV 4, Age of Empire III, Anno, C&C, and WarCraft III. They did not anticipate that we could use Kartograph to own them in these games. This talk shows how we turned the tables on them by using Kartograph to build 0-day cheats. Kartograph is a tool designed to reverse-engineer the memory structure of games, applying analysis and visualization techniques to find small chunks of valuable information within large process footprints (like a needle in a haystack). As a proof of concept, we used Kartograph to extract the relevant 256KB chunks from 1+GB processes and built what is considered the most difficult cheat to build: a map-hack. We will show a live demo of how Kartograph works and some cool cheats we built with it for CIV4, AoE3, Anno, and WarIII. If you want to learn about memory forensic techniques, or if you want to cheat at these popular games, you don't want to miss this talk.

TOKEN KIDNAPPING'S REVENGE

Cesar Cerrudo *Argeniss*

On April 14, 2009 Microsoft released a patch (http://www.microsoft.com/technet/security/bulletin/MS09-012.mspx) to fix the issues detailed in my previous Token Kidnapping presentation (http://www.argeniss.com/research/TokenKidnapping.pdf). The patch properly fixed the issues but...

This new presentation will detail new design mistakes and security issues that can be exploited to elevate privileges on all Windows versions including the brand new Windows 2008 R2 and Windows 7. These new attacks allow to bypass new Windows services protections such as Per service SID, Write restricted token, etc. It will be demonstrated that almost any process with impersonation rights can elevate privileges to Local System account and completely compromise Windows OSs. While the issues are not critical in nature since impersonation rights are required, they allow to exploit services such as IIS 6, IIS 7, SQL Server, etc. in some specific scenarios. Exploits code for those services will be released. The presentation will be given in a very practical way showing how the new issues were found, with what tools, techniques, etc. allowing the participants to learn how to easily find these kind security issues in Windows operating systems

WRT54-TM, MEDIA CENTER AND NETWORK SNIFFER

John A. Colley

Q: Can you build a low budget media center and packet sniffer using a Linksys WT54G-TM in 20 minutes or less?

A: Yes!

Outside the hardware hacks, I'll show you what firmware and packages are needed and get everything operational in less than 20 minutes. It starts with laying the framework by flashing a stock WRT54G-TM and then loading OpenWRT. To finish, I then install and configure the correct packages to auto-mount a 16 Gig SDHC memory chip. We will also get that SDHC card shared on the network for remote access, so we can map a drive to the WRT file system. For even more storage, we will auto mount a network share on the WRT. The final addition will be darkstat installation and configuration for packet sniffing, logging and graphing the network traffic from all the interfaces on the WRT, yes even wireless!

HACKING FACEBOOK PRIVACY

Chris Conley *Technology & Civil Liberties Fellow, ACLU of N. CA*

Facebook's privacy issues are numerous and well-documented, from software "glitches" to decisions that take control away from users. Despite that, it is a still-growing force in the modern Internet and is currently trying to position itself as the gateway to the "social Web" for its 500 million users.

What can we, as hackers, do to protect the privacy of those millions?

This panel walks through a few existing projects that apply software skills to the privacy challenges that Facebook presents, from working within the system using Facebook's Platform API to adding a layer to the system with browser extensions to presenting a robust open-source alternative to the whole Facebook platform. We'll discuss how these different tools fit into various strategies to alter or replace Facebook's existing privacy regime and what other approaches might be successful in protecting privacy on Facebook and other user networks.

OUR INSTRUMENTED LIVES: SENSORS, SENSORS, EVERYWHERE...

Greg Conti *Academy Professor, West Point*

Make no mistake, your analog life is under siege. Virtually every facet of your day to day existence is being sampled, digitized, aggregated, collated, shared, and reality mined. Whether the reason is to support your friendly neighborhood targeted advertiser or to help win a war on terror, a thickening web of sensors tracks our day to day existence in the physical world. Sensors are everywhere: our sneakers, cell phones, appliances, game consoles, power meters, automobiles, highways, bridges, airports, shopping malls and night clubs, among many others. At the same time, technologies that uniquely identify us from a sea of others are on the rise. Financial and other incentives motivate many to start sampling our lives and the law does little to protect us. Convergence of the resultant islands of data is occurring now. More important however is the next step. Because sampling is occurring on a scale never before imaginable, our uniqueness and individuality are giving way to previously impossible models of collective and individual human behavior. How these models will be used is up for debate, but you can be certain they will be abused by some. This talk examines the problem of our impending instrumented existence, studies where it is all going, and provides you with ways to defend yourself, your family, and friends.

PROGRAMMABLE HID USB KEYSTROKE DONGLE: USING THE TEENSY AS A PEN TESTING DEVICE

Adrian Crenshaw *Irongeek.com*

The Programmable HID USB Keystroke Dongle (PHUKD) is a small device based around the Teensy microcontroller development board. It allows users to program in keystrokes and mouse macros that can execute when the device is plugged in, after a set time, or when certain environmental conditions are met (light, noise, temperature, etc.) This device can be used as a replacement for a U3 hacksaw, as a device left behind to execute commands when someone with elevated privileges is likely to be logged in, or give as a Trojan device to unsuspecting targets. Much pwnage should ensue.

IPV6: NO LONGER OPTIONAL

John Curran *President & CEO, ARIN*

The available pool of IPv4 address space has reached a critical level. With about 7% of the IPv4 free pool remaining, organizations should already be taking steps to prepare for IPv6. There is only about a year before IPv4 is fully depleted, so it is vital that all companies adopt IPv6, the next generation of Internet Protocol, now to avoid growth and scaling issues down the road.

While IPv6 will help lead the development and deployment of next-generation, IP-based networks and services, many companies have been slow to adopt IPv6 for various reasons, such as the cost in time and money to move to an IPv6 system, and the need for bridging technology to make IPv4 and IPv6 systems compatible.

In this session, John Curran, CEO of the American Registry for Internet Numbers (ARIN), will describe the key considerations for and benefits of IPv6 adoption and the steps all network operators and engineers should be taking to prepare for IPv4 depletion challenges.

John will also review regional and global IPv4 depletion and IPv6 adoption statistics, address allocation trends, and the IPv6 educational resources available to help operators and engineers prepare.

ARIN is the nonprofit corporation that manages the distribution of Internet number resources, including IPv4 and IPv6 addresses and Autonomous System Numbers (ASNs), to Canada, many Caribbean and North Atlantic islands, and the United States.

FUNCTION HOOKING FOR MAC OSX AND LINUX

Joe Damato

This talk will cover three different methods of function hooking for Mac OSX and Linux. The talk will begin by describing useful bits of Intel64 assembly followed up with 3 different binary rewriting techniques to hook a range of different functions, including some inlined functions, too. We'll finish up with a demo of two nice things that these techniques make possible (a memory profiler and a function call tracer), and one slightly more evil thing.

EXPLOITING INTERNET SURVEILLANCE SYSTEMS

Decius *Security Researcher*

For many years people have been debating whether or not surveillance capabilities should be built into the Internet. Cypherpunks see a future of perfect end to end encryption while telecom companies are hard at work building surveillance interfaces into their networks. Do these lawful intercept interfaces create unnecessary security risks?

This talk will review published architectures for lawful intercept and explain how a number of different technical weaknesses in their design and implementation could be exploited to gain unauthorized access and spy on communications without leaving a trace. The talk will explain how these systems are deployed in practice and how unauthorized access is likely to be obtained in real world scenarios. The talk will also introduce several architectural changes that would improve their resilience to attack if adopted. Finally, we'll consider what all this means for the future of surveillance in the Internet – what are the possible scenarios and what is actually likely to happen over time.

PHYSICAL SECURITY : YOU'RE DOING IT WRONG!

A.P. Delchi *Spiritual Advisor, Attack Research*

Follow in the footsteps of a seasoned geek as he recalls his adventures in the design, buildout, and operation of a physical security system. Learn how to plan ahead for the issues that will fall on your head, how to get vendors to take you to lunch, and how to achieve the impossible : a physical security system that keeps users,management , your budget, and you happy while actually keeping out the bad guys.

THE SEARCH FOR PERFECT HANDCUFFS... AND THE PERFECT HANDCUFF KEYTOOOL

The Open Organization of Lockpickers

The few handcuff talks which have appeared at conferences in the past have focused mostly on how these restraints function and how to open them without a key. While this talk is no exception (going into great detail about the specialized anti-pick protections used by many brands) we will also reveal the product of ongoing, precision research that TOOOL members have conducted.

Did you know that although there is a 'standard' size and shape for basic handcuff keys, every manufacturer has variations, special features, and sizing issues that make creating a single, universal key quite difficult? In our talk, we will explain how to create this type of "ultimate" key that opens all major brands of handcuff, both in the United States and elsewhere around the world. The uber key is verified as working with...

Smith & Wesson (USA)
Peerless (USA)
ASP (USA)
Chicago (USA)
Winchester (USA)
Hiatt-Thompson (UK)
RBS (UK)
Kyoung Chang (Korea)
Yuil (Korea)
Republic Arms (South Africa)
... and more!

We have the math, we have the means, and will demonstrate to everyone how to obtain the best handcuff key you might ever own!

KATANA: PORTABLE MULTI-BOOT SECURITY SUITE

JP Dunning *Founder, Shadow Cave*

Tired of keeping up with dozens of CDs and flash drives loaded with various Live operating systems and applications? I will be introducing the Katana: Portable Multi-Boot Security Suite; which brings many of the best live operating systems and portable applications together onto a single flash drive. Katana includes live distros like Backtrack, the Ultimate Boot CD, UBCD4Win, Ophcrack, and Trinity Rescue Kit as well as hundreds of portable applications like Wireshark, Angry IP, The Sleuth Kit, ClamAV, and OllyDBG. I will cover how Katana was made, what tools are included, how to add additional distributions and applications, and how to use Katana for every day needs.

BREAKING BLUETOOTH BY BEING BORED

JP Dunning *Founder, Shadow Cave*

Bluetooth has come leaps and bounds in its past decade of use. Finding its way into billions of devices world wide. This talk introduces several new Bluetooth attack tools and projects focusing on automated pen-testing, obfuscation, Bluetooth profile cloning, war-nibbling, Denial of Service, and mapping Bluetooth device information. We will be discussing what information your Bluetooth devices gives out about you and what you can do about it, a method for more accurate discovery of Bluetooth devices in non-discoverable mode, how to automate your Bluetooth pen-testing, as well as a few exploits over Bluetooth file transfer.

AN OBSERVATORY FOR THE SSLIVERSE

Peter Eckersley *Senior Staff Technologist, EFF*
Jesse Burns *Founding Partner, iSec Partners*

This talk reports a comprehensive study of the set of certificates currently in use on public HTTPS servers. We investigate who signed the certs, what properties they have, and whether there is any evidence of malicious certificates signed, directly or indirectly, by trusted CAs.

HOW UNIQUE IS YOUR BROWSER?

Peter Eckersley *Senior Staff Technologist, EFF*

This talk reports the results of the panopticlick browser fingerprinting experiment. We show how innocent-looking version and configuration information can be used to uniquely identify almost all desktop browsers, without use of cookies or IP addresses. We discuss how this comes about, how serious a problem it is, and just how hard it will be to fix...

YOUR BOSS IS A DOUCHEBAG... HOW ABOUT YOU?

Luiz "efffn" Eduardo

These days, all hackers have jobs and make some type of money. No matter if you are an independent researcher/ consultant/ 1337 hacker/ or entrepreneur, sometimes you have to deal with the corporate crap, one way or another. Now, how about those who really have to deal with it on a daily-basis in the corporate world? Well, this is an updated version of my DEF CON 15 talk, shorter in time, yet, heavier on rants. Years go by, and most companies still don't understand their employees, and or keep the old style management. On the flip side, the new generation of hackers are getting into good companies, making good money, and some think they reached the peak of their career.

What's up?

We like to blame the companies and bosses, but, how about our own faults and mistakes? You might be part of the problem, not the solution. And those stupid rules you have to follow, might exist because of your actions.

It's easy and common to say your boss is a douchebag, but what happens when YOU become the boss and have to manage the newer (and old) generation? Is it that easy? In addition to just covering the corporate bullshit, I am gonna touch on how some of the cultural differences around the world and try to help the hacker community or the companies to better understand each other.

HACKING WITH HARDWARE: INTRODUCING THE UNIVERSAL RF USB KEYBOARD EMULATION DEVICE – URFUKED

Monta Elkins *Security Researcher*

"If do right, no can defence"—Miyagi

Do you check every USB plug on your computer before you log-in? Didn't think so... URFUKED is used to take over the user's keyboard input and quickly execute preprogrammed attacks with the user's privileges.

Plug in the USB receiver into the victim's computer. Then attack immediately or if necessary wait for the user to login – then trigger the attack remotely with an RF transmitter.

Walk by and talk to the victim, and while he's turned away from the display, press the button on the transmitter to trigger the attack – it'll be done by the time he turns back around. Or trigger it from across the room. It happens too fast to stop even if the user is watching when it happens.

Learn how to build the device cheaply; program it using the opensource Arduino development environment. Learn how to use it and modify it for specific attacks.

BE A MENTOR!

Marisa Fagan *Security Project Manager, Errata Security*

Breaking in to the Information Security field isn't easy. The web of certifications, skills, and credibility is hard to climb through without the help of someone who's been there. Many of us would not be here today without the guidance of a mentor. The Information Security Mentor Match-up program is here at DEF CON to help those people new to the field meet with seasoned pros who know the value of mentoring. Whether you're a researcher, pen tester, network admin, number jockey, hardware hacker, or beer connoisseur, there's someone else at DEF CON that shares your passion. To participate in this session, sign up at http://infosecmentors.com.

HACKING AND PROTECTING ORACLE DATABASE VAULT

Esteban Martínez Fayó *Information Security Researcher at Argeniss*

Oracle Database Vault was launched a few years ago to put a limit on DBAs unlimited power especially over highly confidential data where it is required by regulations. This presentation will show how this add-on product for Oracle Database performs on this difficult task, first giving an introduction to DB Vault and what protections does it brings, then showing with many examples how it is possible to bypass the protections provided. The attacks demonstrated include getting operating system access to disable DB Vault, SQL Injection and impersonation techniques to bypass DB Vault protections and how it is possible using simple exploits to circumvent DB Vault. These attack examples are accompanied by recommendations on how to protect from them. Also the presentation shows some issues with native database auditing and has a section with additional recommendations to secure DB Vault and conclusions.

TROLLING REVERSE-ENGINEERS WITH MATH: NESS... IT HURTS...

frank^2 *Security Engineer*

y = mx+b? f(x) = sin(x/freq)*amp?! SIN X = (A+BX+CX^2)/(P+QX+RX^2)?! None of these formulas as they stand alone really mean much of anything— except maybe a headache for some. Isolating the variables, however, will eventually open the door for us to manipulate our code in creative and exciting ways. This isn't necessarily a ground-breaking technique in obfuscation, but who cares if it's fun? Given an arbitrary formula, we can place our code anywhere we like. It doesn't even need to be a traditional f(x) formula like a sinewave, either— all we need is a number and some constants. Draw your code in circles? Sure! Sexually harass a reverse-engineer by the shape and girth of your code in memory? Hell yes! This talk will attempt to teach a functional method that allows for the random placement, concatenation and manipulation of assembly instructions for the attempt of filling up a reverser's swear jar. You don't need to write any assembly— but you better come knowing its mechanics.

THE ANATOMY OF DRUG TESTING

Jimi Fiekert *MLT(ASCP)*

This talk will cover most of the basics and some of the advanced principles/procedures to how drug screening works. Areas of the subject that will be covered will be the legality of drugs, the legality of drug testing, methods of drug testing, sample types, and reliability.

EXPLOITABLE ASSUMPTIONS WORKSHOP

Joe "Crazy" Foley
Eric "Unlocked" Schmiedl
Zoz

The mental disconnect that occurs in a "limiting assumption" is an excellent opportunity for exploitation. This cognitive security hole makes it possible to identify opportunities for injecting "rootkits" into human-scale systems that won't be found by conventional thinking. Con-men and marketing professionals have already realized the importance of these techniques and use them to great effect. In this workshop, we'll work through a methodology called Axiomatic Design that exposes these assumptions. We will apply this and other techniques to design problems and develop an "assumption-hacker" toolkit that will let you spot and make use of these opportunities.

MASTERING THE NMAP SCRIPTING ENGINE

Fyodor
David Fifield

Most hackers can use Nmap for simple port scanning and OS detection, but the Nmap Scripting Engine (NSE) takes scanning to a whole new level. Nmap's high-speed networking engine can now spider web sites for SQL injection vulnerabilities, brute-force crack and query MSRPC services, find open proxies, and more. Nmap includes more than 125 NSE scripts for network discovery, vulnerability detection, exploitation, and authentication cracking.

Rather than give a dry overview of NSE, Fyodor and Nmap co-maintainer David Fifield demonstrate practical solutions to common problems. They have scanned millions of hosts with NSE and will discuss vulnerabilities found on enterprise networks and how Nmap can be used to quickly detect those problems on your own systems. Then they demonstrate how easy it is to write custom NSE scripts to meet the needs of your network. Finally they take a quick look at recent Nmap developments and provide a preview of what is soon to come. This presentation does not require any NSE experience, but it wouldn't hurt to read http://nmap.org/book/nse.html.

LIVE FIRE EXERCISE: BALTIC CYBER SHIELD 2010

Kenneth Geers *NCIS, CCD CoE*

In May, 2010, the Cooperative Cyber Defence Centre of Excellence in Estonia and the Swedish National Defence College hosted the Baltic Cyber Shield (BCS) international cyber defense exercise (CDX). For two days, six Blue Teams from northern European government, military and academic institutions defended simulated power generation companies against a Red Team of twenty hostile computer hackers. The scenario described a volatile geopolitical environment in which newly hired network security personnel were immediately forced to defend Critical Information Infrastructure (CII) from cyber attacks sponsored by a non-state, terrorist group. This presentation covers the origin and evolution of CDXs and it describes the design, goals, and lessons learned from BCS 2010.

MAKING THE DEF CON 18 BADGE

Joe "Kingpin" Grand

For the fifth year in a row, the DEF CON Badge makes its appearance as a full-fledged, active electronic system. Pushing fabrication techniques to the limit and using some components that are so new they barely exist, the design of this year's badge took some serious risks. Did they pay off? If you're in this talk and not standing in a long line to get your badge, then the answer is "Yes!"

Join Kingpin as he guides you through the entire process of the badge, from initial concept to prototype electronics to firmware design to manufacturing, and all of the problems and challenges he faced along the way.

LEGAL DEVELOPMENTS IN HARDWARE HACKING

Jennifer Granick *Civil Liberties Director, EFF*
Matt Zimmerman *Senior Staff Attorney, EFF*

Hardware hacking raises some novel legal issues This presentation will discuss recent updates in the law that hardware hackers need to know. Topics will include updates on phone unlocking and jailbreaking following the Digital Millennium Copyright Act rulemaking and reverse engineering law. We will also discuss a case in California that will decide whether it's legal for a company to automate user access to her Facebook's data without using the company's APIs.

THE LAW OF LAPTOP SEARCH AND SEIZURE

Jennifer Granick *Civil Liberties Director, EFF*
Kevin Bankston *Senior Staff Attorney, EFF*
Marcia Hofmann *Senior Staff Attorney, EFF*
Kurt Opsahl *Senior Staff Attorney, EFF*

This talk will teach attendees about their legal rights in information stored on their laptops, including when crossing the United States border. We will answer questions such as: What do the police need to do to seize your laptop? Can the U.S. government force you to turn over your password during a border search? Do you have constitutional rights in email and other data stored in the cloud? What happens when the government attempts to force disclosure of passwords? Finally, we will give attendees practical advice on when to do when the police want to take their computers and how to secure device-accessible information, whether on the hard drive or stored remotely.

ADVANCED FORMAT STRING ATTACKS

Paul Haas *Lead Web Application Security Engineer at Redspin, Inc.*

Format string attacks remain difficult in both software and hackademic exercises as the techniques have not improved since their discovery. This session demonstrates advanced format string attack techniques designed to automate the process from creation to compromise as well as incorporate those techniques into the Metasploit framework. The audience is encouraged to bring a basic understanding of format string attacks in order to leave the presentation with the tools necessary to never write one again.

TALES FROM THE CRYPTO

G. Mark Hardy *President, National Security Corporation*

Learn how to crack crypto contests like a pro. The speaker has awarded half a dozen free round-trip plane tickets to previous contest winners. Maybe you'll be next. From the daily newspaper puzzle to badge contests to codes that keep the National Security Agency awake at night, it all comes down to intuition, perspiration, and math skillz.

CONSTRICTING THE WEB: OFFENSIVE PYTHON FOR WEB HACKERS

Nathan Hamiel *Principal Consultant, FishNet Security*
Marcin Wielgoszewski *Security Engineer, Gotham Digital Science*

It seems that everything is a web application nowadays. Whether the application is cloud-based, mobile, or even fat client they all seem to be using web protocols to communicate. Adding to the traditional landscape there is rise in the use of application programming interfaces, integration hooks, and next generation web technologies. What this means for someone testing web applications is that flexibility is the key to success. The Python programming language is just as flexible as today's web application platforms. The language is appealing to security professionals because it is easy to read and write, has a wide variety of modules, and has plenty of resources for help. This additional flexibility affords the tester greater depth than many of the canned tests that come with common tools they use on a daily basis. Greater familiarity plus flexible language equals tester win!

In this presentation we introduce methods with which to create your own clients, tools, and test cases using the Python programming language. We want to put testers closer to the conditions in which they are testing for and arm them with the necessary resources to be successful. We also discuss interfacing with current tools that people commonly use for web application testing. This allows for pinpoint identification of specific vulnerabilities and conditions that are difficult for other tools to identify.

HOW TO HACK MILLIONS OF ROUTERS

Craig Heffner *Senior Security Engineer, Seismic LLC*

This talk will demonstrate how many consumer routers can be exploited via DNS rebinding to gain interactive access to the router's internal-facing administrative interface. Unlike other DNS rebinding techniques, this attack does not require prior knowledge of the target router or the router's configuration settings such as make, model, internal IP address, host name, etc, and does not rely on any anti-DNS pinning techniques, thus circumventing existing DNS rebinding protections.

A tool release will accompany the presentation that completely automates the described attack and allows an external attacker to browse the Web-based interface of a victim's router in real time, just as if the attacker were sitting on the victim's LAN. This can be used to exploit vulnerabilities in the router, or to simply log in with the router's default credentials. A live demonstration will show how to pop a remote root shell on Verizon FIOS routers (ActionTec MI424-WR).

Confirmed affected routers include models manufactured by Linksys, Belkin, ActionTec, Thompson, Asus and Dell, as well as those running third-party firmware such as OpenWRT, DD-WRT and PFSense.

FOE, THE RELEASE OF FEED OVER EMAIL, A SOLUTION TO FEED CONTROVERSIAL NEWS TO CENSORED COUNTRIES

Sho Ho *Telecommunications Specialist, Broadcasting Board of Governors*

Many repressive countries have created Internet censorship systems to prevent Internet users from accessing websites that are deemed inappropriate by their officials. In many cases, these websites are news, political, or religion websites and the main purpose for the ban is to protect the interest of the country's political parties.

FOE is a new censorship circumvention tool developed in-house by the Broadcasting Board of Governors (the Federal Government agency that oversees and supports the operations of Voice of America, Radio Free Asia, Radio Free Europe, and Radio Farda, andRadio, etc.) FOE allows Internet users to get RSS feeds and/or download small files without needing proxy servers. The main goals for the FOE project is to create a multi-platform architecture that allows Internet users to receive unbiased news and to give developers a tool to create new censorship circumvention programs.

HOW TO GET YOUR FBI FILE (AND OTHER INFORMATION YOU WANT FROM THE FEDERAL GOVERNMENT)

Marcia Hofmann *Senior Staff Attorney, EFF*

Want to know the story behind the latest government scandal, or see what a three-letter agency knows about you? In this workshop, the Electronic Frontier Foundation will show you how to use two open government laws, the Freedom of Information Act and the Privacy Act, to ask for records from the federal government. We'll discuss what you can (and can't) get under these laws, how to write an effective open government request, how to appeal an agency's decision to withhold information, and how to figure out next steps.

RIPPING MEDIA OFF OF THE WIRE

HONEY *Network Administrator and Adjunct Professor at John Jay College of Criminal Justice*

The proprietary protocol developed by Adobe Systems for streaming audio, video and data over the Internet, the ëReal Time Messaging Protocol – (RTMP) and the proprietary protocol created by Macromedia used for streaming video and DRM, – Encrypted Real Time Messaging Protocol – (RTMPE) implementations for MySpace use security through obscurity and actually provide zero security.

This talk will describe methods and demonstrate how to download media from MySpace directly and convert the media into MP3s, breaking the DRM by manipulating the RTMP/RTMPE protocol implementation.

Additionally, the talk will describe methods and demonstrate how to download media from YouTube directly and convert the media into MP3s, without using online third parties for conversions, by manipulating parameters in URLs.

PHYSICAL COMPUTING, VIRTUAL SECURITY: ADDING THE ARDUINO MICROCONTROLLER DEVELOPMENT ENVIRONMENT TO YOUR SECURITY TOOLBOX

Leigh Honeywell *co-founder and director of HackLab.TO*
Follower *co-founder of Spacecraft*

The Arduino microcontroller platform entered the world under the guise of "physical computing" aimed at designers and artists but just like you can use a paint brush to jimmy open a door, you can use the Arduino in your security toolkit too. Attend this talk to learn how the Arduino makes microcontrollers and embedded hardware accessible to hax0rs too. After a quick tour through the Arduino ecosystem we'll move on to offensive uses. You'll learn about the potential for use in re-implementing classic attacks, potential vulnerabilities in the "internet of things" infrastructure, USB driver fuzzing, physical control and perhaps some social engineering as well.

DECODING RECAPTCHA EXPLOIT

Chad Houck
Jason Lee

Due to the prevalence of spammers on the internet CAPTCHAs have become a necessary security measure. Without a CAPTCHA in place a system is incapable of knowing whether a human or an automated computer is executing a request. Currently one of the most widely implemented versions of this system is Google's reCAPTCHA due to its robustness thus far. This paper illustrates techniques to defeat this system which has been trusted to secure websites such as Twitter, Facebook, Craigslist, and many others, as well as methods to secure it further. The efficacy of the techniques outlined herein is at a very conservative figure of ten percent, which is more than enough for an applicable exploitation of the system.

THE CHINESE CYBER ARMY – AN ARCHAEOLOGICAL STUDY FROM 2001 TO 2010

Wayne Huang *CTO, Armorize Technologies*
Jack Yu *Senior Security Analyst, Armorize Technologies*

Operation Aurora, GhostNet, Titain Rain. Reactions were totally different in the US and in Asia. While the US media gave huge attention, Asia find it unbelievable and interesting, that cyber warfare and government-backed commercial espionage efforts that have been well established and conduced since 2002, and have almost become a part of people's lives in Asia, caused so much "surprise" in the US.

Here we'll call this organization as how they've been properly known for the past eight years as the "Cyber Army," or "Wang Jun" in Mandarin. This is a study of Cyber Army based on incidences, forensics, and investigation data since 2001. Using facts, we will reconstruct the face of Cyber Army (CA), including who they are, where they are, who they target, what they want, what they do, their funding, objectives, organization, processes, active hours, tools, and techniques. Examples of incidences studies will include, for example, recent intrusions into United Nations and CSIS. Our data was collected over a long period of time, through intelligence trading, and through our involvement in helping Asian governments in their investigation efforts.

Attendees will gain a good understanding of the Chinese Cyber Army, including:

A. Who they are
B. Where they are
C. Who they target
D. What they want
E. What they do
F. Their funding, objectives, organization, processes, and active hours
G. Their tools, and techniques
H. The threat and the countermeasures

DRIVESPLOIT: CIRCUMVENTING BOTH AUTOMATED AND MANUAL DRIVE-BY-DOWNLOAD DETECTION

Wayne Huang *CTO, Armorize Technologies*

This year saw the biggest news in Web security ever—Operation Aurora, which aimed at stealing source code and other intellectual properties and succeeded with more than 30

companies, including Google. Incidence response showed that the operation involved an IE 0-day drive-by-download, resulting in Google's compromise and leak of source code to jump points in Taiwan. The US Government is so concerned that they issued a demarche to the Chinese government.

Using real, live examples, we will show how easy it is to exploit injection-based, XSS-based, and CSRF-based vulnerabilities in FaceBook, Google, Digg, LinkedIn, and other popular websites, and inject drive-by downloads.

If drive-bys are so easy to inject into high-traffic websites, then the question becomes, how easy it is to make them undetectable by automated malware scanning services (such as Google's) and by human manual inspection? We will demonstrate how easy it is to defeat automated detection mechanisms and overview commonly used techniques.

We will reveal for the first time, in this conference, some very advanced techniques that are almost impossible to overcome by automated analysis in the past, now, and in the future. We will release Drivesploit, a drive-by download exploit framework implemented on top of Metasploit. We will go into depth on two particular techniques supported by Drivesploit's a) javascript obfuscation based on behavior-based fingerprinting, and b) javascript timelock puzzles. We will have live demos to show how this technique easily defeats both automated AND manual detection.

At the very beginning of our talk, we will be giving out a digg.com page, which we have infected with a drive-by download created with Drivesploit. Visiting this page with the right browser will trigger the exploit and download a malware that steals browser cookie files. The whole process will be undetectable by antivirus. The actual javascript drive-by code contains a secret phrase. We will give out an ipad to whomever from the audience that is able to correctly deobfuscate the javascript and give out the secret phrase.

Finally, we will present case studies on systems and processes that the largest organizations have put in place in order to fight against Web-based malware. We will also present case studies of our incidence response efforts with organizations hit by Web malware injections such as Google's aurora incident. Based in Taiwan, Co-speaker Wayne has been personally involved in such incidence response efforts since the late 90's.

All source codes related to POC exploits against FaceBook, Google, Digg, LinkedIn, etc, as well as source code of Drivesploit, will be released as open source at the conference.

Attendees will gain the following:

1. Understanding of drive-by downloads and associated terminologies.
2. Information about various drive-by download infection vectors.
3. Appreciation of tools helpful for drive-by analysis, including Malzilla, spikermonkey, rhino, burp and wepawet
4. Realize why drive-by downloads are hard to analyze and detect. Why antivirus fail, why behavior-based approaches fail, and why even manual efforts are difficult
5. Learning the Drivesploit framework and how it can be used to develop poc drive-bys
6. Learning two new deadly techniques: behavior-based browser fingerprinting and javascript timelock puzzles
7. Learning how to implement above two using Drivesploit to defeat both automated and manual drive-by analysis
8. Knowledge about the available countermeasures to this threat

OBOX ANALYZER: AFTERDARK RUNTIME FORENSICS FOR AUTOMATED MALWARE ANALYSIS AND CLUSTERING

Wayne Huang *CTO, Armorize Technologies*
Jeremy Chiu *Security Researcher, Armorize Technologies*

For antivirus vendors and malware researchers today, the challenge lies not in "obtaining" the malware samples – they have too many already. What's needed is automated tools to speed up the analysis process. Many sandboxes exist for behavior profiling, but it still remains a challenge to handle anti-analysis techniques and to generate useful reports.

The problem with current tools is the monitoring mechanism – there's always a "sandbox" or some type of monitoring mechanism that must be loaded BEFORE malware execution. This allows malware to detect whether such monitoring mechanisms exist, and to bail out thus avoiding detection and analysis.

Here we release Obox—an afterDark analyser that loads AFTER malware execution. No matter how well a piece of malware hides itself, there will be runtime forensics data that can be analyzed to identify "traces" of a process trying to hide itself. For example, evidences within the process module lists or discrepancies between kernel – and user-space datastructures. Since analysis is done post mortem, it is very hard for malware to detect the analysis.

By using runtime forensics to extract evidences, we turn a piece of malware from its original binary space into a feature space, with each feature representing the existence or non-existence of a certain behavior (ex, process table tampering, unpacking oneself, adding hooks, etc). By running clustering algorithms in this space, we show that this technique not only is very effective and very fast at detecting malware, but is also very accurate at clustering the malware into existing malware families. Such clustering is helpful for deciding whether a piece of malware is just a variation or repacking of an existing malware family, or is a brand new find.

Using three case studies, we will demo Obox, compare Obox with Obox with recent talks at BlackHat and other security conferences, and explain how Obox is different and why it is very effective. Obox will be released at the conference as a free tool.

EXPLOITING DIGITAL CAMERAS

Oren Isacson *Exploit Writer and Researcher, Core Security Technologies*
Alfredo Ortega *PhD candidate, ITBA*

In this talk we present how to reverse-engineering Canon Powershot digital cameras and take control of most of them to exploit interesting security threats. We present a novel attack method that allows taking control of a digital camera through a compromised memory card. This is a realistic attack scenario, as using the card in unsecured PCs is a

common practice among many users. This attack vector leaves users of digital cameras vulnerable to many threats including privacy invasion and those targeting the camera storage (e.g., deletion and ransomware).

To implement the attack we abuse testing functionalities of the in-factory code. We will show how to analyze the code running in the camera's CPUs and find the parts relevant to the attack. We further show how to debug an emulated copy of the firmware in QEMU.

In contrast with firmware-modding projects like CHDK, our method doesn't require as much user interaction or firmware modification, and our techniques are mostly model-independent.

Finally, we show same proof-of-concept attacks launched from the camera to PCs.

JACKPOTTING AUTOMATED TELLER MACHINES REDUX /EXPLOIT

Barnaby Jack *Director of Research, IOActive Labs*

The presentation "Jackpotting Automated Teller Machines" was originally on the schedule at Black Hat USA 2009. Due to circumstances beyond my control, the talk was pulled at the last minute. The upside to this is that there has been an additional year to research ATM attacks, and I'm armed with a whole new bag of tricks.

I've always liked the scene in Terminator 2 where John Connor walks up to an ATM, interfaces his Atari to the card reader and retrieves cash from the machine. I think I've got that kid beat.

The most prevalent attacks on Automated Teller Machines typically involve the use of card skimmers, or the physical theft of the machines themselves. Rarely do we see any targeted attacks on the underlying software.

Last year, there was one ATM; this year, I'm doubling down and bringing two new model ATMs from two major vendors. I will demonstrate both local and remote attacks, and I will reveal a multi-platform ATM rootkit. Finally, I will discuss protection mechanisms that ATM manufacturers can implement to safeguard against these attacks.

BLACK OPS OF FUNDAMENTAL DEFENSE: WEB EDITION

Dan Kaminsky

Lets be honest: Year in, year out, we keep finding the same bugs in the same places, and wondering: Why don't they learn? Why don't developers use these beautiful tools we provide them — parameterized queries, XSRF tokens, X.509 certificates, and escapes in all their glorious forms? I will tell you: It is because these tools are not very good. And they are not very good, because their quality simply has not mattered. Security demands, devs implement, and if devs don't implement, security complains. And six months later, it's the same bugs, in the same places, by the same devs. It doesn't have to be this way. In this talk, I will discuss the theory that most classes of security flaws are actually symptoms of deeper causes. Furthermore, I will present attempts at addressing these causes. Specific areas of investigation will include potential answers to questions, specifically: 1) Why can't we keep code and data separate? 2) Why can't we log into web sites? 3) Why can't we authenticate across organizational boundaries? By answers, I mean code, and by code, I mean _a lot_ of code. I will not provide any assurances that the code is secure — only extended peer review can do that — but I want to show another way of doing things. This talk is going to be packed with live demos.

HOW I MET YOUR GIRLFRIEND

Samy Kamkar

How I Met Your Girlfriend: The discovery and execution of entirely new classes of Web attacks in order to meet your girlfriend.

This includes newly discovered attacks including HTML5 client-side XSS (without XSS hitting the server!), PHP session hijacking and random numbers (accurately guessing PHP session cookies),

browser protocol confusion (turning a browser into an SMTP server), firewall and NAT penetration via Javascript (turning your router against you), remote iPhone Google Maps hijacking (iPhone penetration combined with HTTP man-in-the-middle), extracting extremely accurate geolocation information from a Web browser (not using IP geolocation), and more.

POWERSHELL...OMFG

David Kennedy (ReL1K) *Hacker*
Josh Kelley (Winfang) *Hacker*

Powershell is as close to a programming language we are going to get through a command line interface on Windows. The ability to perform almost any task we want through Windows is a huge benefit for systems administrators... and hackers. During this presentation we'll be releasing a new attack vector through Powershell that allows you to deliver whatever payload you want to through Powershell in both a bind and reverse type scenario and drop any executable. In addition, we will also be releasing a brand spanking new Metasploit module that incorporates the new attack method. This presentation is focused on showing the security implications and concerns with Powershell and how we may be seeing a lot more attacks on something that has generally not been a focus for discussion. Powershell... omfg.

HARDWARE BLACK MAGIC: DESIGNING PRINTED CIRCUIT BOARDS

Dr. Fouad Kiamilev *Professor, U of Delaware*
Corey 'cOre' Lange *Graduate Student, U of Delaware*
Stephen 'afterburn' Janansky *Senior Computer Engineer, U of Delaware*

Two years ago we hacked some circuits. Last year we showed you how to build things with FPGAs. This year you're in for a real treat – we're going to pull it all together. Up until now you've been limited to demo kits and pre-made packages. You've bought your Arduino, your MSP430, your HCS08, and connected a bunch of nonsense to it to make really cool things – and we've seen some really cool things! Now it's time to learn another skill in the art of hardware black magic: printed circuit board design. It's time to make your own shields, your own kits, and your own neighborly belt buckles! Like last year we're going to demystify the process to you and help you get on track to build you own boards!

This tutorial will go through the process of showing everybody exactly how easy PCB fabrication can be. Starting from an initial circuit design we will take you through all the steps needed to have that new device sitting in your hand. We'll explain all about data sheets, footprints, design rules, verification, taping out, why you need that cap between Vcc and Gnd, silkscreens, layers and much, much more. Several different software packages will be demonstrated to give the audience a wide spread of options to choose from. The audience will be encouraged to follow along as they like. For our use case we'll show you how to build the circuits from the DEF CON 17 badge starting from scratch. This should help those hacking the badge get a better idea of what they're working with. As those who have come to our talks before know, we will have lots of surprises to give away as always! Since we are running a workshop, it is encouraged that you bring your own laptop. We will distribute VIRTUALBOX images with all the software you need to follow along with us.

MALWARE MIGRATING TO GAMING CONSOLES: EMBEDDED DEVICES, AN ANTIVIRUS-FREE SAFE HIDEOUT FOR MALWARE

Ki-Chan Ahn *Hanyang University, Student*
Dong-Joo Ha *Security Researcher at AhnLab, Inc.*

A large portion of people who possess a Gaming Console or a Smartphone are downloading paid software illegally from the web or p2p.

Most of those people do not even give a second thought before installing the downloaded software, and merely just check that the application works. The sense of security here comes from the application's popularity (many people use it = safe) and the fact that the application is working as advertised with no noticeable problems (app is working = nothing is wrong).

The reason why people have this kind of false sense of security for Console Gaming systems or Mobile Devices is because they are not fully aware that malware can potentially bring the same devastating effects as that of a PC malware, and no one has published a reliable way to inject a malware to a legit software.

However, the boundary of these devices and the PC is getting very thin due to the evolution of hardware, which makes these devices capable of bringing the same negative effects of PC malware. Also, most recent Gaming Consoles contain hardware to connect to the network so an almost ideal environment is provided for malware to survive and perform its job.

For instance, you are playing your favorite game Guitar Hero and a malware is silently running in the background attacking another PC in the network stealing sensitive material, as well as luring people to fake sites collecting personal information. It is also possible to use the malware's capability to your advantage, and walk into a company that does not allow you to bring Smartphones or Laptops with a Nintendo DS, and use NDS to connect to the corporate's internal network.

These problems are not only restricted to Gaming consoles or Smartphones but also other various embedded devices. There are already TVs and Cars that have networking capabilities and have Android installed on them. The number of these kind of devices will continue to grow.

In this presentation, we will show how these innocent devices can misbehave and pose a serious threat(in particular Wii, NDS, iPhone, and Android), and show a demo of a malware in live action. We will also show some possible defenses to these kind of attacks.

HARDWARE HACKING FOR SOFTWARE GUYS

Dave King *Security Researcher*

Hardware hacking is cool, but it can be daunting to software guys. Microcontrollers mix hardware and software basically allowing software guys to do hardware in software. Lately several products have emerged that make it even easier for software guys to get hardware up and working.

Arduinos are relatively cheap, open source, all-in-one prototyping boards with a strong community behind them. All you need is a USB cable and the Arduino IDE (which is also open source). The Arduino language is easy to learn for anyone with even a basic knowledge of coding. Arduinos can be made into many different security devices including keyboard emulators, RFID readers/writers, combination lock brute forcing robots, magnetic stripe card emulators, and automated cell phone dialers. In a way, an Arduino is kind of like the hardware equivalent of scripting languages. They make development quick and are a good fit for many projects.

In this talk you'll see examples of projects built with Arduinos and information on how they were done. You'll also see some limitations of Arduinos and some alternatives to typical Arduinos. In the end you'll see that anyone can make really cool hardware, even without a degree in electrical engineering.

TRAINING THE NEXT GENERATION OF HARDWARE HACKERS — TEACHING COMPUTER ORGANIZATION AND ASSEMBLY LANGUAGE HANDS-ON WITH EMBEDDED SYSTEMS

Andrew Kongs *Undergraduate TA in Electrical Engineering*
Dr. Gerald Kane *Dept. Chair in Electrical Engineering*

Hardware hacking can be lots of fun but can be very intimidating getting started. Andrew Kongs and Dr. Gerald Kane wanted to spread the hardware hacking culture to others and saw incoming college engineering freshman as the perfect crowd to indoctrinate. They developed a set of hardware and software tools to help their incoming students play with low-level software and embedded systems.

After sharing the tools with their student audience, they want to share the tools they built with everyone so that those interested can get their feet wet. Want to learn more about the nitty gritty of how microcontrollers and how embedded systems tick (and how to break them) without diving in eyeballs deep? So do many people and the guys from the University of Tulsa are here to help.

DCFLUX IN: MOON-BOUNCER

Matt "DCFluX" Krick *Chief Engineer, New West Broadcasting Systems, Inc.*

This presentation will look at ways you can get critical data across the country during a wired infrastructure break down, Including taking over satellites, low altitude wifi via weather balloons, and bouncing signals off the moon. We will also take a look at some other stuff you can blame us for as time permits.

LIKE A BOSS: ATTACKING JBOSS TOOL

Tyler Krpata

JBoss is an open source Java EE application server. Its default configuration provides several insecure defaults that an attacker can use to gather information, cause a denial of service, or even execute arbitrary code on the system.

AIR TRAFFIC CONTROL INSECURITY 2.0 EXPLOIT

Righter Kunkel *Security Researcher*

This presentation will be a follow up to my "Air Traffic Control: Insecurity and ADS-B" talk last year. I will give a quick overview of what has changed since last year. I will cover a few insecurity's today. How bad is your network when the FAA requires firewalls between critical flight systems and passengers surfing the web on the new 787 plane. I give a caution to all the executive jet owners that it will be much easier to track flights. As always, I want to open peoples eyes to the insecurity of the ATC system.

THE POWER OF CHINESE SECURITY

Anthony Lai *Security Researcher*
Jake Appelbaum *Security Researcher*
Jon Oberheide *University of Michigan*

If you visit China, I am sure you would like the Great Wall, however, if you surf the Internet in China, I am sure you hate the Great FireWall (GFW). How a firewall could "serve" over 3.8 billion Internet users in China is a readily interesting story for the globe.

In the presentation and seminar, we will quote case studies and discussions from various forums in China about how Internet

censorship impacts them. In addition, we will present technical aspects and diagnosis on how censorship could be achieved on the Internet, content filtering software and instant messenger. Moreover, some tools/software (China or non-China made) used to bypass Internet and content censorship.

This presentation is suitable to those would like to do business/tours in China.

BYPASSING SMART-CARD AUTHENTICATION AND BLOCKING DEBITING: VULNERABILITIES IN ATMEL CRYPTOMEMORY-BASED STORED-VALUE SYSTEMS

Jonathan Lee
Neil Pahl

Atmel CryptoMemory based smart cards are deemed to be some of the most secure on the market, boasting a proprietary 64-bit mutual authentication protocol, attempts counter, encrypted checksums, anti-tearing counter measures, and more. Yet none of these features are useful when the system implementation is flawed.

Communications were sniffed, protocols were analyzed, configuration memory was dumped, and an elegant hardware man-in-the-middle attack was developed. From start to finish, we will show you how concepts learned from an introductory computer security class were used to bypass the security measures on a Cryptomemory based stored value smart card laundry system, with suggestions on how things can improve.

BLITZABLEITER – THE RELEASE

Felix "FX" Lindner *Recurity Labs*

The talk presents a simple but effective approach for securing Rich Internet Application (RIA) content before using it. Focusing on Adobe Flash content, the security threats presented by Flash movies are discussed, as well as their inner workings that allow such attacks to happen. Some of those details will make you laugh, some will make you wince. Based on the properties discussed, the idea behind the defense approach will be presented, as well as the code implementing it and the results of using it in the real world.

After a year of development, we hope to release a working tool to the world, so you can apply the defense technique to your web browser.

THESE AREN'T THE PERMISSIONS YOU'RE LOOKING FOR /EXPLOIT

Anthony Lineberry *Security Researcher, Lookout Mobile Security*
David Richardson, Sr. *Software Engineer, Lookout Mobile Security*
Tim Wyatt *Principal Software Engineer, Lookout Mobile Security*

The rise of the robot revolution is among us. In the past year Android has stepped up to become a leader in the world of mobile platforms. As of early may the platform has surpassed the iPhone in market share at 28%. Third party trackers for the Android Market have reported upwards of 50,000 apps available now. The Android security model relies heavily on its sandboxed processes and requested application permissions. It survived the recent pwn2own slay fest unscathed, but this does not mean it is safe by any means. We aim to explore novel techniques for attacks based around abuse of the permission system. Both in performing operations sans appropriate permissions, as well as abusing granted permissions outside of their scope. We'll be demonstrating various ways to hijack input, steal sensitive information, and many other ways to break the rules put in place by our new robot overlords.

MULTIPLAYER METASPLOIT: TAG-TEAM PENETRATION AND INFORMATION GATHERING

Ryan Linn

Sharing information in team penetration testing environments is frequently a challenge. There are a number of tools out there that allow wiki style submissions but any time that data needs to be used, it must be copied and pasted out of one form into another. Metasploit has a robust database with much of the data that a security professional may need to perform new tasks, as well as to check on the status of where the team is as a whole. This presentation will discuss how to share information using Metasploit, how to get data in and out of Metasploit remotely, and how to build and expand tools to automatically store new findings in the database. This presentation will have demonstrations using remote Nmap scanning as well as demonstrate how to write your own tools to manipulate Metasploit data.

REPELLING THE WILY INSIDER

Matias Madou *Security Researcher, Fortify Software*
Jacob West *Security Researcher, Fortify Software*

Working with more than 50 malicious backdoors written over the last 10 years we show how insiders who write code, whether they are developers working for an enterprise or contributors to an open source project, have an almost unlimited number of ways to put chinks in the armor of their software. These holes are often put in place for seemingly good reasons to facilitate easy debugging, make working from home easier, or as a failsafe in case other mechanisms for interfacing with the system fail. However, we'll consider what happens when insiders aren't so pure of heart, including logic bombs and backdoors that allow them to embezzle funds, steal private information, or exact revenge if they become disgruntled.

Whether unintentional or malicious, code that performs questionable behavior or permits unauthorized access can be introduced with relative ease and can persist in a code base almost indefinitely without being discovered. Until it's too late. In this talk, we discuss obvious techniques defenders should employ, outline obvious techniques attackers will apply, and the theoretical limits of the problem. We give detailed examples of insider threats that have been uncovered in real software systems, outline possible motives for malicious insiders, and discuss how external stimuli like layoffs are increasing the attention paid to insider threats. We conclude the talk with the head-to-head results of a face-off between modern static analysis and the best backdoors we've come across.

APP ATTACK: SURVIVING THE MOBILE APPLICATION EXPLOSION

Kevin Mahaffey *CTO, Lookout (formerly Flexilis)*
John Hering *CEO, Lookout (formerly Flexilis)*

The mobile app revolution is upon us. Applications on your smartphone know more about you than anyone or anything else in the world. Apps know where you are, who you talk to, and what you're doing on the web; they have access to your financial accounts, can trigger charges to your phone bill, and much more. Have you ever wondered what smartphone apps are actually doing under the hood? We built the largest-ever mobile application security dataset to find out.

Mobile apps have grown tremendously both in numbers and capabilities over the past few years with hundreds of thousands of apps and billions of downloads. Such a wealth of data and functionality on each phone and a massive proliferation of apps that can access them are driving a new wave of security implications. Over the course of several months, we gathered both application binaries and meta-data about applications on the most popular smartphone platforms and built tools to analyze the data en masse. The results were surprising. Not only do users have very little insight into what happens in their apps, neither do the developers of the applications themselves.

In this talk we're going to share the results of our research, demonstrate a new class of mobile application vulnerability, show how we can quickly find out if anyone in the wild is exploiting it, and discuss the future of mobile application security and mobile malware.

CHANGING THREATS TO PRIVACY: FROM TIA TO GOOGLE

Moxie Marlinspike *Institute For Disruptive Studies*

A lot has changed since discussions around digital privacy began. The security community won the war for strong cryptography, anonymous darknets have been successfully deployed, and much of the communications infrastructure has been decentralized. These strategies were carefully conceived while planning for the most dystopian visions of the future imaginable, and yet somehow they've fallen short of delivering us from the most pernicious privacy threats today. Rather than a centralized state-backed database of all our movements, modern threats to privacy have become something much more subtle, and perhaps all the more sinister. This talk will explore these evolving trends and discuss some interesting solutions in the works.

SEARCHING FOR MALWARE: A REVIEW OF ATTACKERS' USE OF SEARCH ENGINES TO LURE VICTIMS

Dave Maynor *CTO/cofounder, Errata Security; and Research Scientist for Barracuda Labs, Barracuda Networks*
Dr. Paul Judge *Chief Research Officer & VP Cloud Services, Barracuda Networks*

For many people, the first page they visit online is a search engine; in fact, in the US alone more than 14 billion searches per month happen on Google, Yahoo! and Bing. These searches are then siphoned into thousands of popular search terms that are ripe for attackers to exploit. Attackers understand the number of eyeballs and browsers that are at stake and have targeted their attacks against popular search engine results in order to reach the broadest audience possible. For the past five months, Barracuda Labs has been observing and measuring attackers' use of search engine results to host malware or redirect users to malicious sites, collecting data multiple times a day and checking for malicious content around the clock across Google, Yahoo!, Bing and Twitter. In this talk, we reveal statistical data about the search engines and terms that were most targeted. We will highlight key attacker trends, and examine the ability of traditional security approaches like anti-virus and URL filters to react to the rapid movements by the SEO poisoning attacks.

HACKING .NET APPLICATIONS AT RUNTIME: A DYNAMIC ATTACK

Jon McCoy *Software Engineer*

What do you do when you get inside of a .Net program? This presentation will demonstrate taking full advantage of the .Net world from the inside. Once inside of a program don't just put in a key-logger, remold it! I will presentation a how to infiltrate, evaluate, subvert, combine, and edit .Net applications at Runtime. The techniques demonstrated will focus on the modification of core logic in protected .Net programs.

This will make almost every aspect of a target program susceptible to evaluation and change; and allow such hacks as the ability to intermix your favorite applications into a new Frankenstein App, compromise program level security, reverse engineer from memory, modify events, edit the GUI, hunt malware, get the code behind a button, and/or subvert program locks. Demo implementation and tools will be released.

The coding techniques presented will be applicable well beyond compromising the security of a running program. These techniques will grant programmers a new level of access and control over any .Net code, as well as granting the ability to use and integrate with most any .Net application. Creating a development path to test and build 3rd party patches within .Net.

YOU SPENT ALL THAT MONEY AND YOU STILL GOT OWNED...

Joseph McCray *Founder of Learn Security Online*

This talk will focus on practical methods of identifying and bypassing enterprise class security solutions such as Load Balancers, both Network and Host-based Intrusion Prevention Systems (IPSs), Managed Anti-Virus, Web Application Firewalls (WAFs), and Network Access Control Solutions (NAC).

A CHAOSVPN FOR PLAYING CAPTURE THE FLAG

mc.fly, ryd, no _ maam, vyrus

ChaosVPN – the American name is AgoraLink – is a tinc based, fully meshed VPN to connect hackerspaces and other hacker related networks for fun, sharing, learning and competition with each other.

Its purpose is to provide a trusted, private and secure network with high bandwidth, low latency, without single points of failure. The first intended usage of the network was VoIP, but it has become used for lots of different purposes – whatever works on IPv4 and/or IPv6 works on ChaosVPN. This includes our own root zone .hack. Most major Hackerspaces in Europe and America are now connected via the ChaosVPN.

To play CTF contests we decided to build a separate incarnation of this network called warzone. This network is to compete, play and learn in an isolated environment without harming anyone. We host CTF hacking contests and challenges on the network. Critical thinking, source code analysis, reverse engineering and a good understanding of networks are the abilities honed in this environment.

The talk will show the direction ChaosVPN / AgoraLink took and explain some decision points. We will show how it is built, what it does and how to integrate it in your hacker gathering space.

And then we will show how this network can be used to play CTF Games and have some fun.

CYBERTERRORISM AND THE SECURITY OF THE NATIONAL DRINKING WATER INFRASTRUCTURE

John McNabb *President, South Shore PC Services*

The national drinking water infrastructure is vitally important to protection of public health and safety and also supports business, industry, and the national economy. While steps have been taken since 9/11 to identify and mitigate vulnerabilities in the drinking water infrastructure, serious vulnerabilities remain. In this talk, the presenter will discuss and review the challenges of physical and cyber security for the national public drinking water infrastructure and provide his observations, based on 13 years running a local water department and 5 years in IT, on the existing security gaps and what should be done about them. Part of this talk will be based on a talk he gave at the American Water Works Association (AWWA) Water Security Congress in April, 2009 in Washington, DC about a strategic weakness of the national infrastructure. He will also review the state of cyber insecurity of the drinking water infrastructure, the threats currently known to their SCADA systems, and the potential threats and countermeasures that should be considered.

WE DON'T NEED NO STINKIN' BADGES: HACKING ELECTRONIC DOOR ACCESS CONTROLLERS /EXPLOIT

Shawn Merdinger *Security Researcher*

In the security world, attacker physical access often means game over – so what happens if you can't trust your building's electronic door system? This presentation and paper explore attack surfaces and exploitation vectors in a major vendor of electronic door access controllers (EDAC).

The main focus is on time-constrained rapid analysis and bug-hunting methodologies, while covering research techniques that assist in locating and targeting EDAC systems. In addition, a review of practical countermeasures and potential research activities in the EDAC space are covered.

Attendees can expect an eye-opening experience regarding insecurities of critical systems controlling physical access to hospitals, schools, fire stations, businesses and other facilities.

SECURING MMOS: A SECURITY PROFESSIONAL'S VIEW FROM THE INSIDE

metr0 *Senior Software Engineer, Bioware Mythic*

Gold farmers. Cheaters. Beleaguered programmers. All ingredients in a recipe for an unstable, fun-sapping game.

Closely following the model of "Brief Title: Long, Boring Description," Securing MMOs: A Security Professional's View From the Inside will give attendees a look at the security problems plaguing the MMO industry and how modern engineers are taking the fight to cheaters and hackers in MMOs.

LETTING THE AIR OUT OF TIRE PRESSURE MONITORING SYSTEMS

Mike Metzger *Owner, Flexible Creations*

Since 2008 every new car sold in the US requires some type of Tire Pressure Monitoring System be installed. The most popular uses simple unencrypted RF communications to relay the tire pressure information back to the car ECU. This talk goes over the basic history, implementation, and most importantly the unforeseen issues with privacy and subversion of TPM systems

KIM JONG-IL AND ME: HOW TO BUILD A CYBER ARMY TO DEFEAT THE U.S.

Charlie Miller *Principal Analyst, Independent Security Evaluators*

Think you might ever be "asked" by a dictator of an Axis of Evil country to take down the USA in a cyberwar? Ever wonder how someone who finds vulnerabilities and breaks into computers for a living would approach cyberwar, i.e. not Richard Clarke? Then this is the talk for you! In this talk, I outline how to construct a cyber army to attack a developed country, based on my experience as a penetration tester and security researcher. This will highlight anticipated costs, resources needed, roles of individuals, and numbers of people needed, as well as tactics and strategies to use. It will also outline time required to get the unit operational as well as time frames to achieve particular objectives. That's right, the USA is going down!

HD VOICE – THE OVERDUE REVOLUTION

Doug Mohney *Editor-in-Chief, HD Voice News*

After kicking around on the back shelf for years, HD voice is finally gaining traction both in the broadband world and the cellular. And the French are leading the way!

The audio standards for a POTS (Plain Old Telephone System) call have been frozen since about 1937. Since then, modern society has had FM radio, Dolby Sound, TV, HDTV, cell phones, satellite broadcast, the Internet, fiber optics, but no improvement to a stock voice phone call.

Information will include more precisely defining WTF HD voice is, where it is taking place around the globe, the emerging War of the Codecs, mobile vs broadband, enterprise vs consumer, the goodness of HD voice over POTS, and whatever other questions come up from the audience.

GETTING SOCIAL WITH THE SMART GRID

Justin Morehouse
Tony Flick *Principal, FYRM Associates*

Littered with endless threats and vulnerabilities surrounding both social networking and the Smart Grid, the marriage of these two technologies is official, despite protests by the security community. Consumers love it because they can brag to their friends about how green they are. Businesses love it more because it provides fresh material for their marketing departments. Hackers love it the most because it opens up attack vectors, both new and old. During this presentation we dissect readily available social Smart Devices, examining where they get things right, and where they fail. We expand on the failures, discussing and demonstrating attacks against consumers (think PleaseRobMe.com), the Smart Devices themselves, and the social networking sites they communicate with. We want consumers, device manufactures, and social networking sites to understand how to get social with the Smart Grid securely, and prevent social networking privacy from becoming even more complex. The tools we release during this presentation will allow consumers to review their Smart Devices' social footprint, and provide device manufacturers with recommendations that can be implemented immediately. Attendees will leave our presentation armed with a deep understanding of the strengths and weaknesses of social Smart Devices, how to attack their current weaknesses and leverage their current strengths, and utilize our tools to further research how we all can better secure the social side of the Smart Grid.

DEF CON SECURITY JAM III: NOW IN 3-D?

David Mortman *Director, Operations and Security - C3, LLCr*
Rich Mogull *Securosis*
Chris Hoff *Director of Cloud & Virtualization Solutions, Cisco Systems*
Rsnake *ha.ckers.org*
Dave Maynor *Errata*
Larry Pesce *Paul.com*

They say third time is the charm. Some of the biggest mouths in Information Security are back again and once again, we will show you all new of security FAIL. Our panelists will demonstrate innovative hacking techniques in naked routing, web application (in)security, and wireless goats. After taking a sabbatical year, we are also proud to announce that Chris "Squirrel" Hoff will be keeping the rest of us honest with his real-time snarkage. Speaking of real time, moderator David Mortman will be making waffles (and maybe pizzelles) on stage as rewards for best comments, questions and shared fail.

WARDRIVING THE SMART GRID: PRACTICAL APPROACHES TO ATTACKING UTILITY PACKET RADIOS

Shawn Moyer *Principal Security Consultant, FishNet Security*
Nathan Keltner *Security Consultant, FishNet Security*

If you haven't just emerged from a coma, you probably have some idea of the multifaceted attack surface that the inevitable modernization of power transmission and distribution is rapidly introducing

What you may *not* be thinking about just yet, though, is the path much of that attack surface travels on... The air around you

Our talk gives a crash course in the brain-melting number of wireless Smart Grid radio implementations very quickly popping up all around us (some built on actual standards, some snuggled in the comforting blanket of proprietary obscurity) and describes our own experience in reverse engineering Smart Grid radio stacks, and how it's possible to gnaw one's way through to the soft, squishy SCADA underbelly, invariably hiding just below the surface

Along the way, we'll take a hard look at the future landscape of theft of service, point out some larger threats, and try to find a realistic middle ground between the "we're doomed" and the "let's all put our toasters on the Internet" camps in what ultimately is (warts and all) a natural and inevitable step forward.

OPEN SOURCE FRAMEWORK FOR ADVANCED INTRUSION DETECTION SOLUTIONS TOOL

Patrick Mullen *Principal Vulnerability Researcher, Sourcefire, Inc.*
Ryan Pentney *Research Analyst, Sourcefire, Inc.*

Razorback is the result of extensive research by members of the Sourcefire Vulnerability Research Team into developing a platform to address advanced detection problems. The level of sophistication currently demonstrated both by actors described as the 'Advanced Persistent Threat' (APT) and publicly available exploit frameworks such as Metasploit, CANVAS and Core Impact leave increasingly fewer options to provide robust detection. This project is designed to provide enterprise defense teams with a framework for developing the kinds of detection necessary to combat these threats.

A complicating factor in high-CPU-cost detection is the desire of organizations to have low-latency analysis at wire speed. While components of the Razorback system will be able to block first-strike attacks prior to delivery, some detection solutions will cause sufficient latency as to make this impossible. One of the key points of the system is to accept that some solutions require trading real-time blocking for high-accuracy detection.

The Razorback Framework addresses these issues by providing a core infrastructure that matches declared data types to the individual capabilities of various detection systems. By providing an open, documented API, arbitrary data sources can be paired with one or more arbitrary detection systems to provide detection solutions that would otherwise be impossible due to limited data access or restriction on system resources.

This talk will discuss the concepts, design, and architecture of the Razorback Framework as well as introduce several modules for performing advanced inspection, detection, and alerting of network events. Additionally, the capability to update network defense mechanisms based upon these events will be demonstrated. The current implementation of the framework uses a stripped-down version of snort as a data collector, but any data collection engine could be used, including server-based modules designed to work with squid, procmail,or any other proxy or server.

At the conclusion of this discussion, participants will have the knowledge required to install and configure the framework and existing modules and have enough information about the design and philosophy of the framework to begin development on new, custom modules necessary to fill their needs.

THE GAMES WE PLAY

Brandon Nesbit *Security Consultant, Trustwave SpiderLabs*

An in depth forensic analysis of video games and the systems they're played on. The goal of which is to identify the types of information useful to a forensics investigation and any other bits of personal information.

FPGA BITSTREAM REVERSE ENGINEERING TOOL

Lang Nguyen *Security Researcher*

FPGAs are a hot topic at the last few DEF CONs, but we have not seen much talk of hacking FPGAs. In this talk, we present two tools: one to decompile bitstreams into netlists, and one to decompile netlists into Verilog code. For those not familiar with FPGA internals, we will discuss how they work and their bitstream formats. It is highly recommended that attendees know at least some digital electronics/logic design basics.

ANTIQUE EXPLOITATION (AKA TERMINATOR 3: POINT ONE ONE FOR WORKGROUPS)

Jon Oberheide *CTO, Scio Security*

Just as the Terminator travels back from the future to assassinate John Connor using futuristic weaponry, we will travel a couple decades back in time to attack a computing platform that threatens the future of Skynet: Windows 3.11 for Workgroups! Come enjoy the hilarity that ensues when applying modern attack tools and exploitation techniques to an operating system that is approaching its 20th birthday yet EOL'ed only two years ago. We'll be presenting a number of 0-days for applications that are over 6000 days old and poppin' 16-bit calculators all over the place!

EXPLOITSPOTTING: LOCATING VULNERABILITIES OUT OF VENDOR PATCHES AUTOMATICALLY

Jeongwook Oh *Sr. Security Researcher, WebSense Inc.*

This is a new methods to expedite the speed of binary diffing process. Most of the time in analyzing security patches are spent in finding the patched parts of the binary. In some cases one patch contains multiple patches and feature updates. The mixed patches will make the analysis very difficult and time consuming. That's where our new security patch recognizing technology kicks in. We're presenting general signature based security patch recognition and also a method combined with static taint analysis. With both methods implemented, we are presenting new DarunGrim 3 in this year's DEF CON. It'll be a must have tool for the security researchers who's looking for the free 1-day exploits.

ELECTRONIC WEAPONRY OR HOW TO RULE THE WORLD WHILE SHOPPING AT RADIO SHACK

TW "Mage2" Otto *Security Researcher*

This talk will cover alternative weapons. The focus will mostly be on electrical energy based attacks that would target computer and electrical systems. Things like EMP, Injection of noise into electrical systems through a few methods such as RF and direct line injection. It covers how the devices work on a low level with a basic run through on the major components, what they are and what they do. It will cover what these tools/weapons do on a low level as to show what is causing the damage.

It will also cover the design needs for building these tools, and common places to get parts and schematics. The other focus will be on the newer "less than deadly" weapons that are being made for police and law enforcement.

BIG BROTHER ON THE BIG SCREEN: FACT/FICTION?

Nicole Ozer *Technology and Civil Liberties Policy Director, ACLU of Northern CA*
Kevin Bankston *Senior Staff Attorney, EFF*

Can the NSA really do that? Um, yes. Join us at the movies to take a close look at how government surveillance has caught up with the fables dreamed up for Hollywood flicks- from old favorites like Brazil to newer additions like Bourne and Dark Knight. Jaunty tin foil hats and popcorn will be provided!

PRACTICAL CELLPHONE SPYING

Chris Paget *Ethical Hacker*

It's widely accepted that the cryptoscheme in GSM can be broken, but did you know that if you're within radio range of your target you can intercept all of their cellphone calls by bypassing the cryptoscheme entirely? This talk discusses the practical aspects of operating an "IMSI catcher", a fake GSM base station designed to trick the target handset into sending you its voice traffic. Band jamming, rolling LACs, Neighbour advertisements and a wide range of radio trickery will be covered, as well as all the RF gear you'll need to start listening in on your neighbours.

EXTREME-RANGE RFID TRACKING

Chris Paget *Ethical Hacker*

If you think that RFID tags can only be read a few inches away from a reader you haven't met EPC Gen2, the tag that can be found in Enhanced Drivers Licenses - this 900MHz tag is readable from 30 feet with off-the-shelf equipment. Without amplifying the signal from a commercial reader we were able to equal the previous DEF CON record of 69 feet, and with less than $1000 of equipment we achieved considerably further than

that. This talk covers everything you'll need to know to read federally-issued RFID tags at extreme ranges and explores the consequences to personal privacy of being able to do so.

MY LIFE AS A SPYWARE DEVELOPER

Garry Pejski *Security Researcher*

Behold! Billions of computers are infected with spyware every decade! But how! And why!

Let's join our host as he takes you behind the curtain of the mysterious spyware industry. This will be a high level discussion with no technical knowledge needed. I'll be covering how I ended up writing spyware, what the software was capable of, how it was deployed onto millions of machines, how all the money was made (not how you'd expect) and how it all fell apart (of course).

After seeing this talk, all your dreams will come true and you will never die!

"THIS IS NOT THE DROID YOU'RE LOOKING FOR..."

Nicholas J. Percoco *Senior Vice President of SpiderLabs, Trustwave*
Christian Papathanasiou *Security Consultant, Trustwave SpiderLabs*

Android is a software stack for mobile devices that includes an operating system, middleware and key applications and uses a modified version of the Linux kernel. 60,000 cell phones with Android are shipping every day. Android platform ranks as the fourth most popular smartphone device-platform in the United States as of February 2010.

To date, very little has been discussed regarding rootkits on mobile devices. Android forms a perfect platform for further investigation due to its use of the Linux kernel and the existence of a very established body of knowledge regarding kernel-level rootkits in Linux.

We have developed a kernel-level Android rootkit in the form of a loadable kernel module. As a proof of concept, it is able to send an attacker a reverse TCP over 3G/WIFI shell upon receiving an incoming call from a 'trigger number'. This ultimately results in full root access on the Android device. This will be demonstrated (live).

The implications of this are huge; an attacker can proceed to read all SMS messages on the device/incur the owner with long-distance costs, even potentially pin-point the mobile device's exact GPS location. Such a rootkit could be delivered over-the-air or installed alongside a rogue app. Our talk will take participants down this path of development, describing how the PoC was written and laying the foundations for our research to be taken further.

MALWARE FREAK SHOW 2: THE CLIENT-SIDE BOOGALOO

Nicholas J. Percoco *Senior Vice President of SpiderLabs, Trustwave*
Jibran Ilyas *Senior SpiderLabs Forensic Investigator, Trustwave*

We had a busy year. We investigated over 200 incidents in 24 different countries. We ended up collecting enough malware freaks [samples] to fill up Kunstkammer a few times over. Building upon last year's talk, we want to dive deeper and bring you the most interesting samples from around the world - including one that made international headlines and the rest we're positive no one's ever seen before (outside of us and the kids who wrote them). This talk will bring you 4 new freaks and 4 new victims including: a Sports Bar in Miami, Online Adult Toy Store, US Defense Contractor, and an International VoIP Provider. The malware we are going to demo are very advanced pieces of software written by very skilled developers. The complexity in their propagation, control channels, anti-forensic techniques and data exporting properties will be very interesting to anyone interested in this topic.

WIMAX HACKING 2010

Pierce *Security Researcher*
Goldy *Security Researcher*
aSmig *Security Researcher*

It's 2010. WiMAX networks have now been deployed in most major US and European cities. Laptops are being sold with WiMAX built in, and mobile phones are now hitting the market. This talk covers some of the latest findings, public and private, from the wimax-hacking google group. Come see what's been done, what's possible, and what we are working on.

SNIPER FORENSICS - ONE SHOT, ONE KILL

Christopher E. Pogue A.K.A "Big Poppa ReverShell"
Senior Security Consultant, Trustwave SpiderLabs

At one time, computer forensics consisted of pulling the plug, imaging everything in sight, loading those images into EnCase or FTK, and hoping you can "find the bad guy stuff". As computer hackers have become more resourceful, the complexity of computer forensics has likewise increased exponentially. Add to that the growing size of data storage devices, and it becomes infeasible to even consider imaging tens or hundreds of terabytes, let alone load those images into EnCase or some other forensic software. So what's the answer? How can incident responders hope to remain relevant in today's operating environment? With Sniper Forensics!

Live Analysis tools and techniques have exploded onto the incident response scene in the last two years. By gathering and reviewing volatile data and RAM dumps, incident responders can use time proven theories like, "Locard's Exchange Principle", "Occam's Razor", and "The Alexiou Principle" to identify and target only the systems that are part of the breach. What used to take hours of analysis can now be done in minutes! What used to take weeks, can now take days!

By using sound logic and data reduction based on forensic evidence extracted from Live Analysis, incident responders can introduce accuracy and efficiency into their case work at a level not available through any other means. This is truly the cutting edge of modern computer forensics, and not something to be taken lightly! Don't miss the opportunity to learn tips, tools, and hear real world examples of how Live Analysis is literally changing the landscape of modern forensics!

This information is CRITICAL for all incident responders and computer forensic analysts! It combines cutting edge forensic tools and techniques with time proven principles. Successful integration of the material contained in this presentation will without question, reduce the time spent on cases and increase accuracy! It's a targeted approach to forensics which I have dubbed, "Sniper Forensics" rather than the old school, "Shotgun forensics" approach.

INDUSTRIAL CYBER SECURITY

Wade Polk *Instrumentation, Controls & Industrial Cyber Security, WorleyParsons Group Inc.*
Paul Malkewicz
J.Novak

Industrial control systems are flexible constructs that result in increased efficiency and profitability, but this comes at the cost of vulnerability. In past years, industrial cyber security has been mostly ignored due to cost, lack of understanding, and a low incidence rate. More and more these systems rely on commercial, off the shelf software which increases the ease and likelihood of an attack. Today, we face growing threats from individuals, foreign governments and competing companies. The risks have increased by orders of magnitude.

This presentation will provide an overview of control components common to the power industry, common vulnerabilities, the current situation with industry's cyber infrastructure as well as worst case scenarios. A short overview of standards & governances will follow along with suggestions to achieve compliance with overlapping governances. The final phase of the presentation will provide the audience with a case study regarding the security flaws of a programmable logic controller, a common control component, and just how devastating an attack on industrial machinery can be. This will be demonstrated on the physical hardware by simulation of common systems run by this device. After the presentation, a breakout session will occur where the audience will have the opportunity to attempt to compromise the control network.

...-- ..... / .---- .---- / ..-- ..... / .---- ..... / ....- ..--- / ...-- ....- / ...-- ...-- / .---- ..... / ..--- ..... / ....- ...-- / ..--- ..... / ...-- ..... / ...-- .---- / .---- ..... / .---- .---- / ....- ...-- / .---- ..... / ....- .---- / .---- ..... / .---- .---- / .---- ...-- / .---- ---- / ....- ..... / ...-- ..... / ....- / .---- ....- / .---- ..... / ..--- .---- / .---- ...-- / ...-- ..... / ....--

"THIS NEEDS TO BE FIXED" AND OTHER JOKES IN COMMIT STATEMENTS

Bruce Potter *Founder, The Shmoo Group*
Logan Lodge *The Shmoo Group*

Open source. These two words mean lots of things to lots of people. Some say, because it's open source it's more secure because you have complete transparency. Some say, because it's open source it's less secure because amateurs are writing the code. Well, one thing is true, with open source you have free reign to see the code and all the commentary left in there before it's compiled away. Ever wondered what was in those comments? Is there some lingering bug with a comment left behind to remind someone to go back in to fix it later? How many times did the developer leave a comment behind with the word 'bollocks' in it? These are the questions we set out to answer and this talk is about those answers and how we got them.

During our talk we'll cover how we went about crawling the Internets for any and all public repositories, how we parsed the source code and commit statements in the repos we found, how we store the results, and of course the results. Some of what we find will be security specific.... much of what we find will just be comedy. We plan on releasing access to a web interface to perform your own queries against our results to see what interesting comments you can find in which repositories.

TOOLSMITHING AN IDA BRIDGE, CASE STUDY FOR BUILDING A REVERSE ENGINEERING TOOL TOOL

Adam Pridgen *InfoSec Researcher,The Cover of Night*
Matthew Wollenweber *Security Researcher*

The presentation is a case study about an approach to building reverse engineering tools, but in this case, a network bridge between IDA Pro and Debuggers. The presentation will cover the development side of things, and discuss how to leverage open source projects as supplements for code and learning aids, detail

useful sources for this type of development, and provide insight about how to build C++ extensions for WinDbg and IDA, as well as building Python plugins for ImmunityDebugger and VDB.

Additionally, tips and techniques for rapid software development and testing will be described to help aid those onesy/twosy development teams. The target audience for this presentation are those interested in tool development.

BUILD YOUR OWN SECURITY OPERATIONS CENTER FOR LITTLE OR NO MONEY

Josh Pyorre
Chris McKenney

In this talk, I'll use my knowledge of working in a Security Operations Center to provide you with a framework to guide you in building your own SOC or network monitoring system capable of monitoring small to medium sized networks. The goal of this kind of monitoring is to watch for things such as break-in attempts on your network, malware downloads and malware beaconing out after installation and to be a central location for IT security threats. Additionally, the presentation will include some methods of packet analysis of specific events such as cross-site scripting, SQL injection and beaconing malware.

No information on specific technologies or methodologies used by the Security Operations Center Josh works with can be discussed. All information will be based on publicly available tools and information.

IMPROVING ANTIVIRUS SCANNER ACCURACY WITH HYPERVISOR BASED ANALYSIS

Danny Quist *Founder, Offensive Computing*

Modern malware protection systems thoroughly and effectively break modern antivirus software. Simple obfuscations reduce the effectiveness of a scanner, and have been employed by malware authors to stay one step ahead of your AV software. The effect is that they are rendered useless, and you are at more risk. This talk will outline the usage of a hypervisor based deobfuscation engine that greatly improves the effectiveness of AV software. I will show how to make an end-run around some of the tricks that malware authors employ, producing better scanning results and defenses. The techniques we will show are hypervisor analysis, rebuilding imports from the Windows kernel data structures, and a new and improved original entry point detection system. Using techniques inspired by offensive rootkits, we have improved AV detection by as high as 45%.

OPERATING SYSTEM FINGERPRINTING FOR VIRTUAL MACHINES

Nguyen Anh Quynh *AIST (Japan)*

Operating System fingerprinting (OSF) is important to help on deciding security policy enforced on protected Virtual Machine (VM). Unfortunately, current OSF techniques suffer many problems, such as: they fail badly against modern Operating Systems (OS), they are slow, and only support limited OS-es and hypervisors.

This paper analyzes the drawbacks of current OSF approaches against VM in the cloud, then introduces a novel method, named UFO, to fingerprint OS running inside VM. Our solution fixes all the above problems: Firstly, it can recognize all the available OS variants and (in lots of cases) exact OS versions with excellent accuracy, regardless of OS tweaking. Secondly, UFO is extremely fast. Last but not least, it is hypervisor-independent: we proved that by implementing UFO for Xen and Hyper-V.

LORD OF THE BING: TAKING BACK SEARCH ENGINE HACKING FROM GOOGLE AND BING

Rob Ragan *Security Associate at Stach & Liu*
Francis Brown *Managing Partner at Stach & Liu*

During World War II the CIA created a special information intelligence unit to exploit information gathered from openly available sources. One classic example of the team's resourcefulness was the ability to determine whether Allied forces had successfully bombed bridges leading into Paris based on increasing orange prices. Since then OSINT sources have surged in number and diversity, but none can compare to the wealth of information provided by the internet. Attackers have been clever enough in the past to take advantage of search engines to filter this information to identify vulnerabilities. However, current search hacking techniques have been stymied by search provider efforts to curb this type of behavior.

Not anymore. Our demonstration-heavy presentation picks up the subtle art of search engine hacking at the current state and discusses why these techniques fail. We will then reveal several new search engine hacking techniques that have resulted in remarkable breakthroughs against both Google and Bing. Come ready to engage with us as we release two new tools, GoogleDiggity and BingDiggity, which take full advantage of the new hacking techniques.

We'll also be releasing the first ever 'live vulnerability feed', which will quickly become the new standard on how to detect and protect yourself against these types of attacks. This presentation will change the way you've previously thought about search engine hacking, so put on your helmets. We don't want a mess when we blow your minds.

BUILD A LIE DETECTOR/BEAT A LIE DETECTOR

Rain *The Neuronumerous Group*
j03b34r *System Analyst*

Everyone seems to be acquainted with the idea that the polygraph is fallible and that there a million tricks that can supposedly be used to beat it, but how can you really know for sure? One way would be if you pieced together your own polygraph for the singular reason of trying to beat it and we have done just that. We will take a look at the history of deception detection from the birth of Jesus through the Age of Reason to try and get a grasp on how the modern day polygraph came about. Next comes the show and tell on exactly how the group built its own homebrew polygraph and the hilarity that ensues as we tried it out on our friends and family to answer the question; will they beat the machine, or will the machine beat them?

AIRPORT BODY SCANNERS AND POSSIBLE COUNTERMEASURES SEARCH & SEIZURE & GOLFBALLS

Jim Rennie *Attorney*
Eric Rachner *Security Consultant*

In 2008, Eric Rachner was playing a round of Urban Golf with friends in Seattle. When an errant foam ball hit by another player struck a passer-by, the police were called. Eric was standing on the sidewalk minding his own business, and arrested for 'Obstruction' for refusing to identify himself to police. Refusing to back down, Eric took his case to court where it was ultimately dismissed. Today he continues to fight against the Seattle Police, and his story has been featured prominently in local and internet media.

This talk will provide you with a basic understanding of search and seizure law, so that you can appreciate Eric's story and so you know how to exercise your own rights should the time arise. We'll use Eric's situation as a case study in how the rubber meets the road when it comes to the Constitution and interactions with the police.

ENOUGH CYBER TALK ALREADY! HELP GET THIS COLLABORATION ENGINE RUNNING!

Riley Repko *Senior Advisor for Private-Sector Engagements, Office of the Secretary of Defense for Policy, The Pentagon*

With the Private-sector "owning" the intellectual capital for the cyber domain, one key issue is how can we extend the reach of the military's arm to leverage our requirements process, the awareness to existing or the 'art of the possible' cyber capabilities, and finally, 'non-standard' models in acquisition of cyber services? How do we capture/manage cyber cross-domain capabilities to "what's out there" in the private sector that are mutually beneficial to both the military operator and innovative company—in real-time (when necessary)? Finally, how do we incentivize your participation to 'wanna' play?!

IMPLEMENTING IPV6 AT ARIN

Matt Ryanczak *Network Operations Manager, ARIN*

Matt Ryanczak, Network Operations Manager at the American Registry for Internet Numbers (ARIN), began deploying IPv6 in production in 2003. Matt has encountered and overcome the common challenges many of you will encounter working with IPv6. ARIN would like to share its IPv6 deployment experiences with you and relay our knowledge of other production IPv6 deployments to help you get a jump start on your own efforts.

Matt will talk in detail about ARIN's deployment, to include information about provider communications, hardware, and software issues. Matt will also address security-related concerns related to IPv6 deployment.

EXPLOITING WEBSPHERE APPLICATION SERVER'S JSP ENGINE

Ed Schaller *Security Researcher*

WebSphere Application Server (WAS), IBM's Java Enterprise Edition (JEE) application server, is one of the leading application servers and is the predominate application server in the financial and insurance sectors. It is also embedded in several of IBM's other products including WebSphere Portal, WebSphere Process Server and WebSphere Message Broker.

In March 2009, IBM released PK81387 which patches a "Possible application source file exposure" in WAS. Detailed explanation of this vulnerability and it's exploitation will be provided including how implementation details such as character encoding and multiple vulnerabilities, some still unpatched, can be orchestrated to provide file and directory exposure inside a applications Web Archive (WAR). In some cases, with common libraries or WAS feature use, these vulnerabilities can be extended to achieve arbitrary code execution resulting in full compromise of the application server.

Exploitation details will be described and use of this vulnerability and others to execute a remote operating system shell will be demonstrated. Source code to the exploit and other tools will be provided.

PRESENTATIONS

SHODAN FOR PENETRATION TESTERS

Michael "theprez98" Schearer *Security Researcher*

SHODAN is a computer search engine. But it is unlike any other search engine. While other search engines scour the web for content, SHODAN scans for information about the sites themselves. The result is a search engine that aggregates banners from well-known services. This presentation will focus on the applications of SHODAN to penetration testers, and in particular will detail a number of case studies demonstrating passive vulnerability analysis including default passwords, descriptive banners, and complete pwnage. For penetration testers, SHODAN is a game-changer, and a goldmine of potential vulnerabilities.

GAMING IN THE GLASS SAFE - GAMES DRM & PRIVACY

Ferdinand Schober *Security Researcher*

"DRM is the new form of slavery - but it also spies on you."

– conversation with a gamer

After years of perceived-rampant piracy on the PC, game publishers are beginning to shackle gamers with increasingly intrusive DRM systems. However, recent game news headlines are brimming with failures of these measures. Cracks either get released weeks prior to street dates, or systems fail and prohibit legitimate buyers from running their games. Even worse, these systems can easily be used to siphon the personal information of gamers and potentially cause them major pain.

This presentation will show an overview of what is out there in the game DRM space and dive into specific issues. These issues detail how game platforms and their DRM systems create a goldmine of personal data and can be easily used to mess with legitimate gamers.

YOU'RE STEALING IT WRONG! 30 YEARS OF INTER-PIRATE BATTLES

Jason Scott *www.textfiles.com*

Historian Jason Scott walks through the many-years story of software piracy and touches on the tired debates before going into a completely different direction - the interesting, informative, hilarious and occasionally obscene world of inter-pirate-group battles. A multi-media extravaganza of threats, CSI-level accusations and evidence trails, decades of insider lingo, and demonstrations of how the more things change, the more they still have to keep their ratios up.

DC 18 MOVIE NIGHT — GET LAMP

Jason Scott *www.textfiles.com*

At the dawn of the era of home computing, an unusual type of game was the most popular to play. With just a screen of text and a prompt, you'd be asked the simple question: WHAT DO YOU WANT TO DO NEXT?

As you typed in commands and sentences, the games would tell you a story, a story fraught with danger, excitement, puzzles and hours of exploration. They were called text adventures, adventure games and interactive fiction. They dominated the sales charts and introduced millions to the power and flexibility of home computers. No other type of computer game could come close. And then they were gone forever... or maybe they never actually left.

GET LAMP tells the story from a cave in Kentucky to the modern era of what some call a brand new form of literature. Director Jason Scott will be on hand for the showing, as well as a Q&A afterwards.

SMART PROJECT: APPLYING RELIABILITY METRICS TO SECURITY VULNERABILITIES

Blake Self *Researcher, S2ERC Security and Software Engineering Research Center*
Wayne Zage *Professor, Computer Science, Ball State University*
Dolores Zage *Computer Science, Ball State University*

Battlefield operations depend heavily on network-centric computing systems. Such complex and widely dispersed operations expose network-based systems to unprecedented levels of reliability and security risks. Computer systems and network security are often limited by the reliability of the software running on constituent machines. Faults in the software expose vulnerabilities, pointing to the fact hat a critical aspect of the computer security problem resides in software. This presentation will be covering the latest results of the Software Engineering Research Center's (SERC) SMART Project. SMART stands for Security Measurement and Assuring Reliability through metrics Technology. SMART is the result of a collaboration between SERC and the US Army Research Laboratory (ARL). Through our previous award winning reliability research and our current focus of analyzing large open-source systems, promising results were obtained to support the accurate prediction of the reliability and security of individual and interdependent components in a network-centric environment. Open-source systems being analyzed include Apache, OpenSSH, OpenSolaris, and Firefox. An analysis of our current methods and results of those methods will be given.

HACKING DOCSIS FOR FUN AND PROFIT

Blake Self *Researcher, S2ERC http://www.serc.net*
Bitemytaco *Researcher*

At DEF CON 16 we showed various modifications and techniques to gain free and anonymous cable modem internet access. During our last talk, the DOCSIS hacking scene was behind the cable companies. Thanks to the efforts of SBHacker and others, we our now ahead of the cable companies. This talk will analyze and discuss the tools, techniques, and technology behind hacking DOCIS 3.0. We will also cover new areas like hacking PacketCable and discuss all of the DOCSIS related arrests since our last speech. We will be releasing the Haxomatic USB JTAG/SPI programmer by Rajkosto & SBHacker and updated DOCSIS 3.0 hacked firmware for TI puma5-based cable modems at this talk.

RIP YOUR BROWSER FOR X06 DAYS

James Shewmaker *Bluenotch Corporation*

All significant modern applications are ported to the web. Even with custom applications, there is at least one web-based component. Web applications are partially dependent on web clients and are continuously part of the security equation. These issues manifest in ways that make the user vulnerable. For example, privacy vulnerabilities are demonstrated with the EFF's Panopticlick browser fingerprinting project. Whether the weakness is privacy exposure, a client exploit, or a server exploit,—an empowered browser can provide a reasonable defense.

This presentation will review three typical vulnerability classes and selected defenses: Privacy, Client-Side, and Server-side. The goal of this new tool is to shorten the vulnerability window to six days. The talk finale will demonstrate how to poison your browser's DOM for anonymity.

HACKING ORACLE FROM WEB APPS

Sumit "sid" Siddharth *Principal Security Consultant, 7safe*

This talk will focus on exploiting SQL injections in web applications with oracle back-end and will discuss all old/new techniques. The talk will target Oracle 9i,10g and 11g (R1 and R2) It is widely considered that the impact of SQL Injection in web apps with Oracle back-end is limited to extraction of data with the privileges of user mentioned in connection string. Oracle database does not offer hacker friendly functionalities such as openrowset or xp_cmdshell for privilege escalation and O.S code execution. Further, as Oracle by design do not support execution of multiple query in single SQL statement, the exploitation is further restricted. The Talk will highlight attack vector to achieve privilege escalation (from Scott to SYS) and O.S code execution, all by exploiting Oracle SQL injections from web applications. Further, as a number of organizations move to compliances like PCI ensuring that the Card data is always stored encrypted with the private key never stored inside the database. The talk will focus on what hackers are doing in the wild to bypass these and to obtain clear text card data when its only stored encrypted or even when its never stored.

WEAPONIZING LADY GAGA, PSYCHOSONIC ATTACKS

Brad Smith *Director, Computer Institute of the Rockies*

This session introduces and demonstrates the emerging attack vector of psychosonics. Attend and you'll understand how to turn ANY MP3 into a weapon, a study aid, a hidden calming session or helping you experience that Ah-Ha moment of discovery simply by injecting an alternate data stream attack made up of psychosonic frequencies

You'll learn how different mental states can be created using frequencies that interact with the brain, how the military is using this attack vector, how Vegas uses these same techniques on customers, which open source software creates these frequency generated psychic states and sites so you can continue your adventures in psychosonics. Multiple new attacks based on psychosonics will be demonstrated and fully explained to you can easily integrated these into you attack tools.

This is an "attack the audience" session where you'll actually experience these psychosonic attacks so you can judge their effectiveness for yourself. Better yet, you'll understand how to incorporate this attack vector into your future attack surface. Hey, psychosonics is much better than the flame thrower bra she already has!

A NEW APPROACH TO FORENSIC METHODOLOGY – !!BUSTED!! CASE STUDIES TOOL

David C. Smith *Georgetown University and HCP Forensic Services*
Samuel Petreski *Georgetown University and Remote IT Consulting*

Imagine the following experiment, a unique case is given to three digital forensic analysts and each is given the opportunity to engage the requester in order to develop the information needed to process the case. Based on the information gathered, each of the three analysts is asked to provide an estimate to complete the investigation and can proceed with up to 20 hours to process the case. The analysts are then measured based on the total findings, the time required to process the case, the initial information gathered, and the estimated time to process the case. The expected result is to be varied based on experience and individual characteristics, such as organization, discipline,

and the attention to detail of each analyst. Imagine this same experiment but with only 8 hours to process the case, because that is the way it happens in real life.

David Smith and Samuel Petreski have developed a methodology that fits within the Analysis phase in one of the standard Digital Forensic Analysis Methodologies - PEIA (Preparation, Extraction, Identification, and Analysis), to provide a structure for consistent results, better development of the requested goals, increase efficiency in fulfilling the goals, and develop an improved estimate of the time required to complete the request.

This methodology involves the generation and validation of case goals, the evaluation of methods used to achieve the goals, a structure for estimating the effectiveness, time required, processing results of specific methods, and generalized organization and time management. The primary goal of this methodology is to address the structure and optimal path that would allow a digital forensic examiner to perform an examination with a high level of efficiency and consistent results.

This presentation provides an introduction to this methodology and applies its key concepts to real sanitized digital investigations, such as tracking down a suspected executive's adult craigslist ad, performing an analysis on a compromised system involving social security numbers, and making the determination of intellectual property theft.

PYRETIC - IN MEMORY REVERSE ENGINEERING FOR OBFUSCATED PYTHON BYTECODE

Rich Smith *Senior Researcher Immunity Inc*

Increasing numbers of commercial and closed source applications are being developed in Python. Developers of such applications are investing more & more to stop people being able to see their source code through a variety of code obfuscation techniques. At the same time Python is an increasingly present component of 'Cloud' technologies where traditional bytecode decompilation techniques fall down through lack of access to files on disk.

The pyREtic presentation discusses the techniques and subsequent toolkit developed while trying to audit one such closed source Python application. The methodology behind the approaches used as well as practicalities of reverse engineering at the Python level (rather than the assembly level that we are all more familiar with) will be discussed as well as releasing a toolkit.

The toolkit is able to reverse Python applications from live objects in memory as opposed to decompiling .pyc bytecode files, it also shows how to defeat the techniques most commonly employed to obfuscate Python code today. This will allow people to find bugs in code that was previously opaque to them.

YOUR ISP AND THE GOVERNMENT: BEST FRIENDS FOREVER.

Christopher Soghoian *Security & Privacy Researcher*

Your Internet, phone and web application providers are all, for the most part, in bed with the government. They all routinely disclose their customers' communications and other private data to law enforcement and intelligence agencies. Worse, firms like Google and Microsoft specifically log data in order to assist the government, while AT&T and Verizon are paid $1.8 million per year in order to provide real time access to customer communications records to the FBI. How many government requests does your ISP get for its customers' communications each year? How many do they comply with? How many do they fight? How much do they charge for the surveillance assistance they provide? Who knows. Most companies have a strict policy of not discussing such topics.

You might assume that the law gives companies very little wiggle room - when they are required to provide data, they must do so. This is true. However, companies have a huge amount of flexibility in the way they design their networks, in the amount of data they retain by default, the emergency circumstances in which they share data without a court order, and the degree to which they fight unreasonable requests.

The differences in the privacy practices of the major players in the telecommunications and Internet applications market are significant: Some firms retain identifying data for years, while others retain no data at all; some voluntarily provide the government access to user data - Verizon even argued in court that it has a 1st amendment right to give the NSA access to calling records, while other companies refuse to voluntarily disclose data without a court order; some companies charge the government when it requests user data, while others disclose it for free. For an individual later investigated by the government, the data retention practices adopted by their phone company or email provider can significantly impact their freedom.

Unfortunately, although many companies claim to care about end-user privacy, and some even that they compete on their privacy features, none seem to be willing to compete on the extent to which they assist or resist the government in its surveillance activities. Because information about each firm's practices is not publicly known, consumers cannot vote with their dollars, and pick service providers that best protect their privacy.

This talk will pierce the veil of secrecy surrounding these practices. Based upon a combination of Freedom of Information Act requests, off the record conversations with industry lawyers, and investigative journalism, the practices of many of these firms will be revealed.

SO MANY WAYS TO SLAP A YO-HO:: XPLOITING YOVILLE AND FACEBOOK FOR FUN AND PROFIT

strace *Security Researcher*

Maybe you've played YoVille because your spouse or relative got you into it. Maybe its your overt obsession or secret delight. If you haven't heard of YoVille, well, its got at least 5 Million active users connected directly with Facebook. This talk explores the Web 2.0 pandora's box that is the trust relationship between YoVille and Facebook.

For many, YoVille is fiercely competitive in a hyper-decorative way, it has its own intricate economics, and yes, tempers can flare when you get rooked by a Scammer. You will meet people you want to pimp slap-really hard-and this talk will show you how. Send a school teacher who you don't like a "Jeffrey Dahmer Snack Plate with fingers and toes".Don't like that History Professor? Send him a Burning Cross that lets him know he is welcome in the neighborhood.

Want to show off for that special someone? You can grant yourself "The YoVille Sexiest Man (or Babe) award, and have it prominently displayed on your Facebook wall for everyone to see, rickrolling anyone who clicks on it..

Or you can embrace the dark side...

Imagine a cute "trojan" Puppy that takes over your system when you click to adopt it? Yes, it can be done — and its going on right now. Post that payload on Facebook or to the YoFeed and mass root everyone who clicks on it? This talk will show you how it is done, as well as recorded examples of actual attacks.

On a more serious tone, when you Click "Accept" and allow YoVille to access Facebook, you introduce a cornucopia of attack vectors for spreading malware within the user population. The origin, authenticity, and integrity of almost any message shared from YoVille can be subverted. If the receiving application trusts that message is safe, it becomes a broadcast for widening the attack.

I will show how a blackhat can use YoVille to spread destructive malware. Anything that updates the Facebook wall or sends a user a hyperlink is susceptible.

These problems are not unique to YoVille and Facebook — this is clearly the tip of a very enormous iceberg. So embrace your dark-side for an hour of YoVillany, and remember:

Never click on "candy" from strangers.

The types of attacks we will demonstrate were collected in the wild, by watching the activities of a Philippine hacker group and then reverse engineering their attacks in our own lab. The real attacks ranged from using YoVille to Spam facebook user walls with ads selling discount meds, as well as spoofed YoVille events or collectibles that pointed to shotgun attacks against the browser.

DECEIVING THE HEAVENS TO CROSS THE SEA: USING THE 36 STRATAGEMS FOR SOCIAL ENGINEERING

Jayson E. Street *CIO, Stratagem 1 Solutions*

There are new threats arising every day. The problem is there has been a vulnerability in the system that has not been patched since the first computer was created by Humans!

As the network perimeter hardens and the controls on the desktop tightens. Hackers are going back to the basics and getting through the firewall by going through the front door. They are bypassing the IPS and IDS simply by bypassing the receptionist.

We look at this topic with a different viewpoint. We look at the history of social engineering from Amenhotep 3 to Sinon of Greece as well as how the culture of the country you're in dictates the strategy to use. All this shown in an offbeat way showing how 1st century strategies can still be used to break into 21st century networks.

SOCIAL NETWORKING SPECIAL OPS: EXTENDING DATA VISUALIZATION TOOLS FOR FASTER PWNAGE

The Suggmeister

If you're ever in a position when you need to pwn criminals via social networks or see where Tony Hawk likes to hide skateboards around the world, this talk is for you.

The talk is delivered in two parts, both of which are intended to shine a fun light on visual social network analysis.

The first part introduces how you can extend the powerful data visualization tool, Maltego to speed up and automate the data mining and analysis of social networks. I'll show how I analyzed skateboard legend, Tony Hawk's twitter hunt and highlight how you could use the same techniques to set up your very own backyard miniature ECHELON.

The second part illustrates how these techniques have been used to enumerate a 419 scam, infiltrate the scammers social network and expose deeper, more sinister links to organized crime.

I focus specifically on Twitter and Facebook, demonstrating how you can graphically map and analyze social relationships using the Twitter API's, publicly available Facebook profiles, screen scraping and some clunky regex."

Related to this talk is the DEF CON Twitter Hunt

Each day at DEF CON you will have an opportunity to blag yourself a sweet limited edition DEF CON-ized skateboard deck. There may also be a couple of signed Tony Hawk decks slung in for good measure too... who knows.

You will have to follow @TheSuggmeister during DEF CON to know where to look. He'll be tweeting clues which lead to prizes. Hashtag #DCTH'

GETTING ROOT: REMOTE VIEWING, NON-LOCAL CONSCIOUSNESS, BIG PICTURE HACKING, AND KNOWING WHO YOU ARE

Richard Thieme *ThiemeWorks, Author and Speaker*

Richard Thieme celebrates speaking for Def Con for fifteen years by discussing the deepest truths he knows and relating them to Big Picture hacking.

Thieme references the most fervent explorations of his life, from immersion in the works of the Society for Psychical Research while living in England as a young man to conversations with remote viewers in the government's Stargate program to thirty years of research in UFO reports (in particular, experiences of "strangeness" such as space-time distortion and telepathic knowledge transfer) to the passionate, obsessive exploits of real hackers and what they discover when boundaries dissolve - all in a context of his own anomalous experiences. He talks about the background for 'Mind Games', his recently published collection of nineteen stories of brave new worlds and alternate realities, which he wrote after a friend at NSA told him, "The only way you can tell the truth now is in fiction". He also discusses why another NSA friend warned that he was 'over the line' in the hall of mirrors as a result of his conversations with dark side actors and victims alike. He weaves all this together in the kind of narrative usually reserved for private conversations but which he feels he owes Def Con colleagues and friends after fifteen years of enthusiastic and mutual knowledge-transfer.

WEB APPLICATION FINGERPRINTING WITH STATIC FILES

Patrick Thomas *Vulnerability Detection Engineer (Qualys)*

Web Application fingerprinting before 2010 has been a hodge-podge of different techniques, usually relying on meta tags or other clues helpfully added by well meaning (but security challenged) developers. Current hardening approaches hamper standard web application fingerprinting, but new static file techniques provide extremely high accuracy and require new hardening approaches. We will discuss implementation details of static file fingerprinting, demonstrate the effectiveness, and release both a fingerprinting tool and a hardening tool to help administrators harden their machines against this approach.

VIRGRAFF101: AN INTRODUCTION TO VIRTUAL GRAFFITI

Tottenkoph *Researcher*

Want to take a stab at graffiti but spray paint fumes get you nauseous? Worry not! The world of virtual graffiti is slowly but surely gaining popularity and now hackers with little to no artistic inclination are able to go out and alter digital media as well as leave messages in virtual mediums with as much (if not more) finesse than our analogue counterparts are able to.

This talk will cover the history of graffiti, how virtual graffiti is different from digital graffiti, examples of virtual graffiti that you can attempt on your own, and the legal implications involved with virtual graffiti. There will also be materials provided for LED throwies.

INSECURITY ENGINEERING OF PHYSICAL SECURITY SYSTEMS: LOCKS, LIES, AND VIDEOTAPE

Marc Weber Tobias *Investigative Attorney and Director, Security Labs*
Tobias Bluzmanis *Director, Security Labs*
Matt Fiddler *Director, Security Labs*

Many lock manufacturers do not understand the relationship and intersection between "mechanical engineering" and "security engineering" in their products. Typically, design engineers are fairly adept at making things work properly, but often fail to contemplate, conceive of, or identify potential or actual "real world" vulnerabilities in the locks and related hardware that they manufacture. This failure can lead to serious breaches in security, often from relatively trivial attacks by unauthorized individuals, rogue employees, and criminals. It can also result in significant liability upon the part facilities that employ specific security technology, and a failure to comply with regulatory requirements.

Issues stemming from insecurity engineering are compounded by intended or unknowing misrepresentations by lock manufacturers about the security of their products. These statements by manufacturers are often relied upon by consumers, commercial enterprises, and the government sector in the decision-making process involving the purchase of security hardware. Ultimately, security relates to both the protection of people and assets, and to liability. Thus, it is imperative that security professionals understand the interrelationship between standards, hardware design, and real-world threats. Marc Tobias, Tobias Bluzmanis, and Matt Fiddler have significant experience and track record in analyzing, discovering, and exposing real-world threats in security hardware. In this presentation, they will address these issues.

ATTACK THE KEY, OWN THE LOCK

Schuyler Towne *Executive Editor, Non Destructive Entry Magazine*
datagram *lockwiki.com & lockpickingforensics.com*

Locks restrict access to anyone lacking the correct key. As security components, we depend on locks to secure our most valuable possessions. Most attacks demonstrated in recent years involve manipulation of the lock components with special picking tools, but what if we focused on using incorrect or blank keys to make a variety of tools? Bumping is a good example, but there are many other ways incorrect or modified keys can be used to defeat locks. Like the cryptography world, physical Keys are vulnerable to attack in even the highest security locks.

This talk focuses on using modified keys and key blanks to open, decode, and bypass several locking mechanisms, including many high security locks. We demonstrate and discuss the security implications of key-based attacks on modern lock designs.

BALANCING THE PWN TRADE DEFICIT

Valsmith *Owner & CEO, Attack Research, LLC*
Colin Ames *Principal Researcher, Attack Research, LLC*
Anthony Lai *Security Researcher*

One of the presenters is a native Chinese language speaker and heavily involved in the Chinese security community and so brings unique insights to this presentation. The other presenters have been analyzing APT style threats for many years and bring this experience to bare on a problem that has received a lot of recent attention, but little technical depth. Viewers should walk away with a greatly increased understanding of the Chinese hacking community as well as some ideas for better defense, and collaboration.

SIE PASSIVE DNS AND THE ISC DNS DATABASE

Paul Vixie *President, Internet Software Consortium & Chairman, ARIN*
Robert Edmonds *Internet Software Consortium*

Passive DNS replication is a technique invented by Florian Weimer for tracking changes to the domain name system. This session will introduce the problems faced by passive DNS replication in the areas of collection, analysis, and storage of DNS data at scale, and will introduce state-of-the-art solutions to these problems developed at ISC SIE. Components of SIE's passive DNS architecture will be showcased, including a specialized DNS capture tool, a tool for processing and deduplicating raw DNS message data, and the storage engine used to archive and index processed data. A bulk HTTP query API and web interface to the storage engine will also be demonstrated and made available.

GO GO GADGET PYTHON! INTRODUCTION TO HARDWARE HACKING

Nick Waite
Furkan Cayci

So you know that embedded devices are everywhere, even attended some talks here about hardware security. Perhaps you've thought how nice it would be to make a linux USB driver for some windows-only device, or you've got something proprietary you would like to reverse-engineer and circuit-bend for your next big scheme. But how does a software person enter the world of circuits? And once you have some circuits, how can you bring the data back into your box?

Bridging the worlds of hardware and software, two electrical engineers will answer your questions while showing you how to pwn some sweet hardware and charm it over the USB port with Python. From our own trials and tribulations building and hacking real devices, from a simple USB missile launcher to a complex biomedical data acquisition system, you will learn about USB packet sniffing, rapid-prototyping device drivers in python, deciphering circuit boards and data sheets for fun & profit, and the use of electrical test equipment. We aim to leave you armed and ready to take on hardware of your own.

BUILD YOUR OWN UAV 2.0 - WIRELESS MAYHEM FROM THE HEAVENS!

Michael Weigand *Cadet, West Point*
Renderman *Researcher, Church of Wifi*
Mike Kershaw *Author of Kismet, Wireless Guru*

Earlier this year the community was shown how to successfully Build your own Predator UAV @ 99.95% Discount - and a recon mission over DC! But now new payloads take the fun/danger to a new level! Come find out how you can not only easily warfly and conduct aerial reconnaissance for your next 'mission' but also use your UAV as a roving angel of wireless death, as always from the confines of your couch.. Or Vegas hotel room.

The presenters will quickly overview how you can build your own UAV drone, and then detail how to outfit it to conduct wireless recon, attack, penetration, and other goodies.. Several demo mission from the Vegas Strip will be presented with video!

THE NIGHT THE LIGHTS WENT OUT IN VEGAS: DEMYSTIFYING SMARTMETER NETWORKS

Barrett Weisshaar *Security Consultant, Trustwave Spiderlabs*
Garret Picchioni *Undergraduate Student, University of Arizona*

Smart meter technology is moving from news PR item to reality in many major utility markets, bringing with it the promise of fewer site visits and lower rates. With these devices, your local utility can perform a variety of actions from starting/stopping service, upgrading your meter, or even shutting off certain 'smart' appliances (air conditioners, etc) during peak demand to avoid brownouts. All of this is accomplished using a wireless network of meters and relay stations to transmit commands, power readings, and the like. But is this network the result of lessons hard learned by previous mistakes in wireless technologies (WiMAX), or do all claims of security rely on a closed system of obscurity (FHSS)?

Armed with the services of a USRP software radio, we set about to probe the underlying structure of the smart meter network and analyze the security (or lack thereof) of the transmission methods. Can your neighbor's 3am parties finally be silenced? Was your service utilization "really" that low for the month? Come to find out!

AN EXAMINATION OF THE ADEQUACY OF THE LAWS RELATED TO CYBER WARFARE

Dondi "SpookDoctor06" West *Security Researcher*

This paper argues that the current rules of war are adequate for addressing the unique issues that are encountered as a result of conducting and defending against cyber warfare. The author begins by giving a survey of the laws that have the biggest impact on cyber warfare. Next, the author describes several paradigms that have come about as a result of cyber warfare, followed by a direct rebuttal. The author then asserts five reasons for why the U.S. should not enter into an international treaty for cyber warfare: (1) combatant commanders already have proper guidelines for conducting warfare; even in the information age; (2) fields of law are seldom demarcated by technology; (3) an unintended consequence of a cyber warfare law is that it may pose an undue limitation on a primarily non-lethal strategic deterrence; (4) our adversaries are unlikely to comply; and (5) the rate of technology growth will outpace the ability for an international cyber regime to produce responsive policy, while the flexibility allotted by the UN Charter and laws of war are able to absorb technological advances. The author concludes that the current UN Charter and Laws of War should continue to govern cyber warfare and that creating an international treaty or law for cyber warfare would do more harm than good and seriously cripple our ability to conduct war.

FROM "NO WAY" TO 0-DAY: WEAPONIZING THE UNWEAPONIZABLE

Joshua Wise *Graduate Student, Carnegie Mellon University*

Many system administrators take a patch for a denial of service attack to be optional. What's the worst that could happen? Oh no — a local user could crash the system. We'll just reboot it; MyPhpGresQL.py on Rails is totally transactional, right? Commit messages fixing these sorts of crashes are often characteristically underreported, too: "allows attackers to cause an application crash".

In some cases, the descriptions are correct; the worst that can happen is that the system will crash. Too often, though, the risk is under-assessed. Although an application may not be vulnerable to a simple stack-smashing buffer overflow, that's not all that an attacker can do! This talk will take a recent Linux kernel CVE for a denial of service attack and weaponize it to privilege escalation.

An understanding of some of the inner workings of the Linux kernel, and of operating system concepts in general, will greatly enhance your experience at this talk, but may not be necessary.

CRAWLING BITTORRENT DHTS FOR FUN AND PROFIT

Scott Wolchok *Graduate Student, University of Michigan*

This talk describes how crawling BitTorrent's DHTs used for distributed tracking can be used for two opposing goals. First, pirates can crawl the DHTs to build BitTorrent search engines in just a few hours without relying on the survival of any existing search engines or trackers. Second, content owners can crawl the DHTs to monitor users' behavior at large scale.

The talk will start by explaining what BitTorrent DHTs are and how they work. Then, it will describe the design of our attacks, how we validated them, and how many torrents and IPs we monitored (over 1 million each). Finally, we'll look at the impact that shifting from centralized BitTorrent tracking to DHTs, as The Pirate Bay has started to do, will have on the BitTorrent arms race.

PWNED BY THE OWNER: WHAT HAPPENS WHEN YOU STEAL A HACKER'S COMPUTER

Zoz

Having your place broken into and your computer stolen can be a nightmare. Getting revenge on the fucker who has your machine can be a dream come true. I had the opportunity to experience both of these when my machine was stolen in Boston and then showed up in Las Vegas 2 years later. Come share some laughs at a lamer's expense, participate in the pwnage, and learn some resulting insights into the implications of certain security decisions.

PANEL: OF BYTES AND BULLETS

Jeffrey Carr *Author, Inside Cyber Warfare: Mapping the Cyber Underworld*
Joseph Menn *Author, Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet*
Robert Vamosi *Author, When Gadgets Betray Us: What We Don't Understand about the Everyday Gadgets We Use and How That Puts Us at Risk*

This authors' panel has all the makings of a page-turning bestseller: crime lords, heroes, spies, global cartels, corporate scandals, hi-tech gizmos, betrayal, revolution, political intrigue, and midnight assassination attempts. As with all good books, it's the characters – the researchers, the criminals, and the victims – and their unique stories that will keep you riveted to your seat.

PANEL: DNS SYSTEMIC VULNERABILITIES AND RISK MANAGEMENT: A DISCUSSION WITH THE EXPERTS

Rod Beckstrom *CEO and President of ICANN*
Dan Kaminsky *Chief Scientist, Recursion Ventures*
Paul Mockapetris *Chairman and Chief Scientist at Nominum*
Ken Silva *Senior VP and Chief Technology Officer, VeriSign*
Mark Weatherford *VP and Chief Security Officer, NERC*

The experts on this panel will provide their views on systemic risks facing the DNS and provide thoughts on measures that should be undertaken to remediate the risks. The panelists will discuss both the challenges and the security benefits that will arise from the implementation of DNSSec.

PANEL: INTERNET WARS

Marcus Sachs *Director, SANS Internet Storm Center*
Kenneth Geers *NCIS, Cooperative Cyber Defence Centre of Excellence*
Dan Kaminsky *Director of Penetration Testing ,IOActive*
Andrew Fried *Ex-IRS*
Paul Vixie *President, Internet Software Consortium & Chairman, ARIN*
John Bumgarner
Daniel Uriah Clemens
John Ives

Continuing our tradition from previous years, leading experts from different industries, academia and law enforcement will be on stage participating in this panel to discuss the current threats online, hazards inside the Internet, battles between low level cyber criminals all the way to the mafia, special agents, spies, and even information warfare between nation-states.

This panel begins with a short introductory presentation on the latest technologies and operations by the Bad Guys and the Good Guys. We will talk about what's going on with Internet operations, global routing, botnets, extortion, phishing and the annual revenue the mafia is getting from it. Then we'll move into question and answers from the audience. Panelists will accept questions on any subject related to the concept of Internet warfare, crime, and espionage, and will discuss it openly in regard to what's being done and what we can expect in the future, both from the Bad Guys and the Good Guys.

Discussion will focus on operational issues currently happening on the Internet, not on vulnerabilities or the latest leet hack you might have heard about. The discussion is mostly technical and operational in nature, but in previous years attendees have asked questions directing the discussion to the legal side of things. Participants are people who are involved with battling cyber crime daily, and many are leaders in the security operations community of the Internet.

Audience members bearing six-packs of beer for the panelists will advance to the front of the line.

BIOPANEL: HACKING THE FUTURE: WEAPONIZING THE NEXT GENERATION

James Arlen
James Costello
Leigh Honeywell
Tim Krabec
Tiffany Rad

Join this panel of "experts" who will discuss, debate, enlighten, and do battle on the topic of Hacker Parenting. From a multitude of viewpoints – paternal, maternal, fictive aunt and victim – the methodologies and techniques of applying the hacker mindset to parenting will be discussed. It is expected that the audience will participate as this topic is one on which everyone has an opinion. Maybe it's possible to do great work and develop a generation of people primed to hack the planet and take over.

MEET THE EFF

Kevin Bankston *Senior Staff Attorney, EFF*
Eva Galperin *Referral Coordinator, EFF*
Jennifer Granick *Civil Liberties Director, EFF*
Marcia Hofmann *Senior Staff Attorney, EFF*
Kurt Opsahl *Senior Staff Attorney, EFF*

Get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This session will include updates on current EFF issues such as Digital Millennium Copyright Act (DMCA) use and misuse (and—maybe—the much delayed exemptions), whether breaking Captchas breaks the law, Digital Due Process (updating

communications privacy law), legal and policy issues with walled gardens, 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.

PCI, COMPROMISING CONTROLS AND COMPROMISING SECURITY

Jack Daniel
Joshua Corman
Dave Shackleford
Anton Chuvakin
Martin McKeay
Alex Hutton
James Arlen

PCI at DEF CON? Are you on drugs? Sadly, no – compliance is changing the way companies "do security", and that has an effect on everyone, defender, attacker, or innocent bystander. If you think all that 0-day you've heard about this week is scary, ask yourself this: if a company accepts credit cards for payment, which is a more immediate threat – failing an audit or the possibility of being compromised by an attacker? That is one of the reasons "they" do not listen to "us" when we try to improve security in our environments – as real as they are, our threats are theoretical compared to failing a PCI assessment. Systems are hardened against audit, not attack. Sadly, this is often an improvement, but this can also reduce security and provide a template for attackers. This panel will discuss and debate strengths and weaknesses of PCI, expose systemic problems in PCI-DSS, and propose improvements.

MEET THE FEDS – POLICY, PRIVACY, DETERRENCE AND CYBER WAR

Mike Convertino *AF*
Jerry Dixon *Ex-DHS*
Andy Fried *Ex-IRS*
Jon Iadonisi *Ex-Navy Seal*
Kevin Manson *Ex-FLETC*
Rich Marshall *DHS*
Marcus Sachs *Ex-DoD, Ex-DHS, Ex-NSC*
Roberta Stempfley *DHS*
Randy Vickers *US CERT*
Lin Wells *NDU*
Amit Yoran *Ex-DHS*

This panel of federal agents will discuss cyber policy. How do we conduct robust continuous monitoring across a large multi-organizational enterprise yet stay within the constitutional requirements for privacy, civil rights and civil liberties? What changes are needed in the criminal justice system to increase the deterrence of committing cyber-crime? Once a cyber-crime has occurred – and through investigative efforts is determined to be a nation state – who becomes in charge or better yet who determines if it rises to the level of cyber-war versus espionage?

MEET THE FEDS – CSI:TCP/IP

Jim Christy *DC3*
Mike Convertino *AF*
Jerry Dixon *Ex-DHS*
John Garris *NASA*
Barry Grundy *Treasury*
Bob Hopper *NW3C*
Ken Privette *USPS IG*
Tom Talleur *Ex-NASA*
Trent Teyema *FBI*

The average criminal case today has over a terabyte worth of data to analyze. The cyber forensics field is just beginning to mature. Join federal agents to discuss the forensics field now and in the future.

PANEL: OCTF: 5 YEARS IN 50 MINUTES

Adam
CP
Frank^2
Jeffball
Merlin
Vyrus

Over the past 5 years oCTF has grown and evolved. Running the contest has been a lot of work, a lot of fun, and educational for both the contestants as well as for us. This panel talk will go over everything from the inspirations which started it back at the Alexis Park, right through to this year when we passed the torch to The Tube Warriors.

Thursday, July 29 Speaking Schedule

	Track 1	Track 4	Capri 111	Capri 112	Capri 113
13:00	**DEF CON 101** Panel	**HACKING THE FUTURE: WEAPONIZING THE NEXT GENERATION** Panel	**GO GO GADGET PYTHON! : INTRODUCTION TO HARDWARE HACKING** Nick Waite, Furkan Cayci	**EXPLOITABLE ASSUMPTIONS WORKSHOP** Joe "Crazy" Foley, Eric "cOre" Lange, Stephen "afterburn" Jahanisky	**HARDWARE BLACK MAGIC: DESIGNING PRINTED CIRCUIT BOARDS** Dr. Fouad Kiamilev, Corey
14:00			**THE KEYS TO RUNNING A SUCCESSFUL DEF CON GROUP BY DC612** David "VideoMan" M. N. Bryan, Jared Bird		
15:00					

Friday, July 30 Speaking Schedule

	Track 1	Track 2	Track 3	Track 4	Track 5
10:00	**KEYNOTE** Top Secret	**SIE PASSIVE DNS AND THE ISC DNS DATABASE** Paul Vixie	**HOW TO GET YOUR FBI FILE (AND OTHER INFORMATION YOU WANT FROM THE FEDERAL GOVERNMENT)** Marcia Hofmann	**WELCOME AND MAKING THE DEF CON 18 BADGE** Dark Tangent, Joe Grand	**OCTF: 5 YEARS IN 50 MINUTES** Panel
11:00	**MEET THE FEDS - CSI:TCP/IP** Panel	**CLOUD COMPUTING, A WEAPON OF MASS DESTRUCTION?** David "VideoMan" M. N. Bryan	**OUR INSTRUMENTED LIVES: SENSORS, SENSORS, EVERYWHERE...** Greg Conti		**OPEN PUBLIC SENSORS AND TREND MONITORING** Daniel Burroughs
11:30					**FOE, THE RELEASE OF FEED OVER EMAIL** Sho Ho

Friday, July 30 Speaking Schedule

	Track 1	Track 2	Track 3	Track 4	Track 5
12:00	DNS SYSTEMIC VULNERABILITIES AND RISK MANAGEMENT: A DISCUSSION Panel	HOW UNIQUE IS YOUR BROWSER? Peter Eckersley	YOUR ISP AND THE GOVERNMENT: BEST FRIENDS FOREVER. Christopher Soghoian	BUILD A LIE DETECTOR/ BEAT A LIE DETECTOR Rain	GOOGLE TOOLBAR: THE NARC WITHIN Jeff Bryner
12:30					CRAWLING BITTORRENT DHTS FOR FUN Scott Wolchok
13:00	MEET THE FEDS - POLICY, PRIVACY, DETERRENCE AND CYBER WAR PANEL	TOKEN KIDNAPPING'S REVENGE Cesar Cerrudo	THE LAW OF LAPTOP SEARCH AND SEIZURE Jennifer Granick, Kevin Bankston, Marcia Hofmann, Kurt Opsahl	HOW HACKERS WON THE ZOMBIE APOCALYPSE Dennis Brown	WHO CARES ABOUT IPV6? Sam Bowne
13:30					OPERATING SYSTEM FINGERPRINTING FOR VMS Nguyen Anh Quynh
14:00	ENOUGH CYBER TALK ALREADY! HELP GET THIS COLLABORATION ENGINE RUNNING! Riley Repko	LORD OF THE BING: TAKING BACK SEARCH ENGINE HACKING FROM GOOGLE AND BING Rob Ragan, Francis Brown	SEARCH & SEIZURE & GOLFBALLS Jim Rennie, Eric Rachner	BUILD YOUR OWN UAV 2.0 - WIRELESS MAYHEM FROM THE HEAVENS! Michael Weigand, Renderman, Mike Kershaw	WEB APP. FINGERPRINTING WITH STATIC FILES Patrick Thomas
14:30					WRT54-TM, MEDIA CENTER AND NETWORK SNIFFER John A. Colley
15:00	OPEN LETTER - CALL TO ACTION	TALES FROM THE CRYPTO G. Mark Hardy	EXPLOITING INTERNET SURVEILLANCE SYSTEMS Decius	EXPLOITING DIGITAL CAMERAS Oren Isacson, Alfredo Ortega	AIR TRAFFIC CONTROL INSECURITY 2.0 Righter Kunkel
15:30					FPGA BITSTREAM REVERSE ENGINEERING Lang Nguyen

16:00	OF BYTES AND BULLETS Panel	EXPLOITING WEBSPHERE APPLICATION SERVER'S JSP ENGINE Ed Schaller	HACKING FACEBOOK PRIVACY Chris Conley	VIRGRAFF101: AN INTRODUCTION TO VIRTUAL GRAFFITI Tottenkoph	LIKE A BOSS: ATTACKING JBOSS Tyler Krpata
16:30					LETTING THE AIR OUT OF TIRE PRESSURE MONITORING SYSTEMS Mike Metzger
17:00	MASTERING THE NMAP SCRIPTING ENGINE Fyodor, David Fifield	HACKING ORACLE FROM WEB APPS Sumit Siddharth	AN OBSERVATORY FOR THE SSLIVERSE Peter Eckersley, Jesse Burns	DCFLUX IN: MOON-BOUNCER Matt Krick	EVILGRADE, YOU STILL HAVE PENDING UPGRADES? Francisco Amato
17:30					TRAINING THE NEXT GEN. OF HARDWARE HACKERS Andrew Kongs, Gerald Kane
18:00	MEET THE EFF Kevin Bankston, Eva Galperin, Jennifer Granick, Marcia Hofmann, Kurt Opsahl	DRIVESPLOIT: CIRCUMVENTING BOTH AUTOMATED AND MANUAL DRIVE-BY-DOWNLOAD DETECTION Wayne Huang	BAD MEMORIES Elie Bursztein, Baptiste Gourdin, Gustav Rydstedt	WEAPONIZING LADY GAGA, PSYCHOSONIC ATTACKS Brad Smith	BE A MENTOR! Marisa Fagan
18:30					YOUR BOSS IS A DOUCHEBAG... HOW ABOUT YOU? Luiz "efffn" Eduardo
19:00	BLACK OPS OF FUNDAMENTAL DEFENSE: WEB EDITION Dan Kaminsky	HACKING AND PROTECTING ORACLE DATABASE VAULT Esteban Martínez Fayó	FOCA2: THE FOCA STRIKES BACK Chema Alonso, José Palazón "Palako"	GETTING ROOT Richard Thieme	ANTIQUE EXPLOITATION Jon Oberheide
19:30					PWNED BY THE OWNER Zoz
20:00			BIG BROTHER ON THE BIG SCREEN: FACT/FICTION? Nicole Ozer, Kevin Bankston	LIVE FIRE EXERCISE: BALTIC CYBER SHIELD 2010 Kenneth Geers	
21:00				PANEL: INTERNET WARS Marcus Sachs	

Saturday, July 31 Speaking Schedule

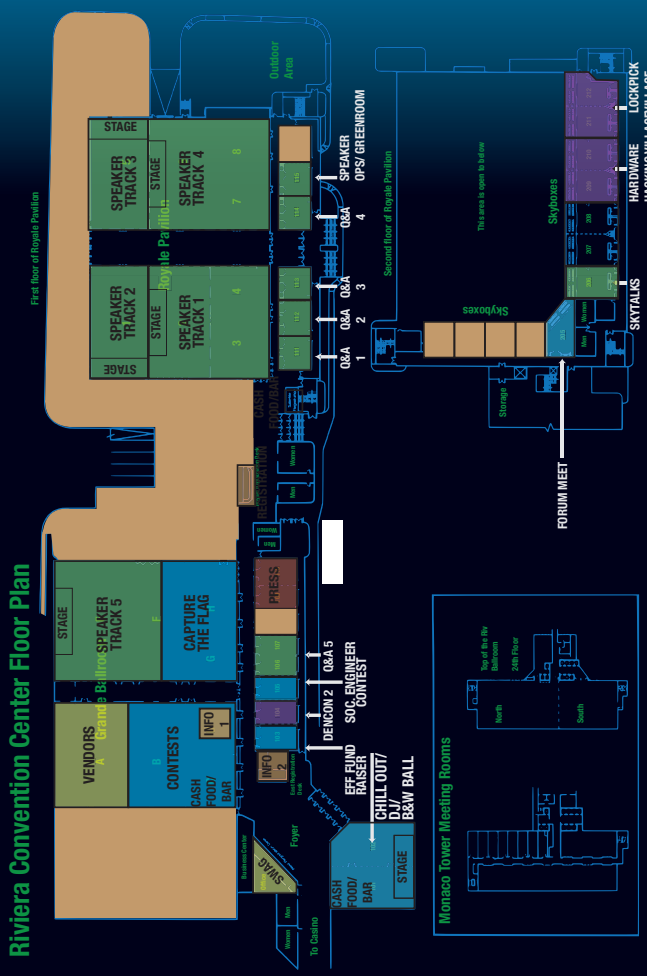
	Track 1	Track 2	Track 3	Track 4	Track 5
10:00	LEGAL DEVELOPMENTS IN HARDWARE HACKING Jennifer Granick	EXPLOITING SCADA SYSTEMS Jeremy Brown	CHANGING THREATS TO PRIVACY: FROM TIA TO GOOGLE Moxie Marlinspike	EXTREME-RANGE RFID TRACKING Chris Paget	IMPROVING ANTIVIRUS SCANNER ACCURACY WITH HYPERVISOR BASED ANALYSIS Danny Quist
11:00	APP ATTACK: SURVIVING THE MOBILE APPLICATION EXPLOSION Kevin Mahaffey, John Hering	KIM JONG-IL AND ME: HOW TO BUILD A CYBER ARMY TO DEFEAT THE U.S. Charlie Miller	MASSEXPLOITATION Michael Brooks	JACKPOTTING AUTOMATED TELLER MACHINES REDUX Barnaby Jack	SEARCHING FOR MALWARE: A REVIEW OF ATTACKERS' USE OF SEARCH ENGINES TO LURE VICTIMS David Maynor
12:00	"THIS IS NOT THE DROID YOU'RE LOOKING FOR..." Nicholas J. Percoco, Christian Papathanasiou	CYBER[CRIME|WAR] CHARTING DANGEROUS WATERS Iftach Ian Amit	THIS NEEDS TO BE FIXED, AND OTHER JOKES IN COMMIT STATEMENTS Bruce Potter, Logan Lodge	INSECURITY ENGINEERING OF PHYSICAL SECURITY SYSTEMS: LOCKS, LIES, AND VIDEOTAPE Marc Weber Tobias, Tobias Bluzmanis, Matt Fiddler	KATANA: PORTABLE MULTI-BOOT SECURITY SUITE JP Dunning
13:00	PRACTICAL CELLPHONE SPYING Chris Paget	THE POWER OF CHINESE SECURITY Anthony Lai, Jake Appelbaum, Jon Oberheide	TROLLING REVERSE-ENGINEERS WITH MATH: NESS... IT HURTS... frank^2	BYPASSING SMART-CARD AUTHENTICATION AND BLOCKING DEBITING Jonathan Lee, Neil Pahl	FROM "NO WAY" TO 0-DAY: WEAPONIZING THE UNWEAPONIZABLE Joshua Wise
14:00	HD VOICE - THE OVERDUE REVOLUTION Doug Mohney	WARDRIVING THE SMART GRID: PRACTICAL APPROACHES TO ATTACKING UTILITY PACKET RADIOS Shawn Moyer, Nathan Keltner	PYRETIC - IN-MEMORY REVERSE ENGINEERING FOR OBFUSCATED PYTHON BYTECODE Rich Smith	WE DON'T NEED NO STINKIN' BADGES: HACKING ELECTRONIC DOOR ACCESS CONTROLLERS Shawn Merdinger	MALWARE MIGRATING TO GAMING CONSOLES: EMBEDDED DEVICES, AN ANTIVIRUS-FREE SAFE HIDEOUT FOR MALWARE Ki-Chan Ahn, Dong-Joo Ha
15:00	THESE AREN'T THE PERMISSIONS YOU'RE LOOKING FOR Anthony Lineberry, David Richardson, Sr., Tim Wyatt	SCADA AND ICS FOR SECURITY EXPERTS: HOW TO AVOID CYBERDOUCHERY James Arlen	WPA TOO! Md Sohail Ahmad	PHYSICAL SECURITY : YOU'RE DOING IT WRONG! A.P. Delchi	MY LIFE AS A SPYWARE DEVELOPER Garry Pejski
16:00	MOBILE PRIVACY: TOR ON THE IPHONE AND OTHER UNUSUAL DEVICES Marco Bonetti	THE NIGHT THE LIGHTS WENT OUT IN VEGAS: DEMYSTIFYING SMARTMETER NETWORKS Barrett Weisshaar, Garret Picchioni	HOW TO HACK MILLIONS OF ROUTERS Craig Heffner	DECEIVING THE HEAVENS TO CROSS THE SEA: USING THE 36 STRATAGEMS FOR SOCIAL ENGINEERING Jayson E. Street	MALWARE FREAK SHOW 2: THE CLIENT-SIDE BOOGALOO Nicholas J. Percoco, Jibran Ilyas
17:00	RESILIENT BOTNET COMMAND AND CONTROL WITH TOR Dennis Brown	CYBERTERRORISM AND THE SECURITY OF THE NATIONAL DRINKING WATER INFRASTRUCTURE John McNabb	SHACKING DOCSIS FOR FUN AND PROFIT Blake Self, bitemytaco	PHYSICAL COMPUTING, VIRTUAL SECURITY Leigh Honeywell, follower	HACKING .NET APPLICATIONS: A DYNAMIC ATTACK Jon McCoy
18:00	RIPPING MEDIA OFF OF THE WIRE HONEY	THE CHINESE CYBER ARMY - AN ARCHAEOLOGICAL STUDY FROM 2001 TO 2010 Wayne Huang, Jack Yu	ADVANCED FORMAT STRING ATTACKS Paul Haas	HACKING WITH HARDWARE: URFUKED Monta Elkins	BLITZABLEITER – THE RELEASE Felix "FX" Lindner
19:00	YOU'RE STEALING IT WRONG! 30 YEARS OF INTER-PIRATE BATTLES Jason Scott	AN EXAMINATION OF THE ADEQUACY OF THE LAWS RELATED TO CYBER WARFARE Dondi West	CONNECTION STRING PARAMETER ATTACKS Chema Alonso, José Palazón "Palako"	PROGRAMMABLE HID USB KEYSTROKE DONGLE: USING THE TEENSY AS A PEN TESTING DEVICE Adrian Crenshaw	DEF CON SECURITY JAM III: NOW IN 3-D? Panel
20:00		INDUSTRIAL CYBER SECURITY Wade Polk, Paul Malkewicz, J. Novak			

Sunday, August 1 Speaking Schedule

	Track 1	Track 2	Track 3	Track 4	Track 5
10:00	THE SEARCH FOR PERFECT HANDCUFFS... AND THE PERFECT HANDCUFF KEY TOOOL	MULTIPLAYER METASPLOIT: TAG-TEAM PENETRATION AND INFORMATION GATHERING Ryan Linn	BROWSER BASED DEFENSES James Shewmaker	WEB SERVICES WE JUST DON'T NEED Mike "mckt" Bailey	WIMAX HACKING 2010 Pierce, Goldy, aSmig
11:00	ATTACK THE KEY, OWN THE LOCK Schuyler Towne, datagram	BALANCING THE PWN TRADE DEFICIT Valsmith, Colin Ames, Anthony Lai	CONSTRICTING THE WEB: OFFENSIVE PYTHON FOR WEB HACKERS Nathan Hamiel, Marcin Wielgoszewski	IPV6: NO LONGER OPTIONAL John Curran	HARDWARE HACKING FOR SOFTWARE GUYS Dave King
12:00	PCI, COMPROMISING CONTROLS AND COMPROMISING SECURITY Jack Daniel	POWERSHELL...OMFG David Kennedy (ReL1K), Josh Kelley	REPELLING THE WILY INSIDER" Matias Madou, Jacob West	EXPLOITATION ON ARM – TECHNIQUE AND BYPASSING DEFENSE MECHANISMS Itzhak "zuk"" Avraham	ELECTRONIC WEAPONRY OR HOW TO RULE THE WORLD WHILE SHOPPING AT RADIO SHACK Mage2
13:00	HOW I MET YOUR GIRLFRIEND Samy Kamkar	BUILD YOUR OWN SECURITY OPERATIONS CENTER FOR LITTLE OR NO MONEY Josh Pyorre	THE ANATOMY OF DRUG TESTING Jimi Fiekert	IMPLEMENTING IPV6 AT ARIN Matt Ryanczak	CHAOSVPN FOR PLAYING CTFS mc.fly, ryd, vyrus, no _ maam
14:00	DECODING RECAPTCHA Chad Houck	SECCUBUS - ANALYZING VULNERABILITY ASSESSMENT DATA THE EASY WAY... Frank Breedijk	A NEW APPROACH TO FORENSIC METHODOLOGY - !!BUSTED!! CASE STUDIES David C. Smith, Samuel Petreski	BREAKING BLUETOOTH BY BEING BORED JP Dunning	THE GAMES WE PLAY Brandon Nesbit
15:00	SO MANY WAYS TO SLAP A YO-HO:: XPLOITING YOVILLE AND FACEBOOK FOR FUN AND PROFIT strace	TOOLSMITHING AN IDA BRIDGE, CASE STUDY FOR BUILDING A REVERSE ENGINEERING TOOL" Adam Pridgen	OPEN SOURCE FRAMEWORK FOR ADVANCED INTRUSION DETECTION SOLUTIONS Patrick Mullen, Ryan Pentney	SMART PROJECT: APPLYING RELIABILITY METRICS TO SECURITY VULNERABILITIES Blake Self, Wayne Zage, Dolores Zage	KARTOGRAPH : FINDING A NEEDLE IN A HAYSTACK Elie Bursztein, Jocelyn Lagarenne, Dan Boneh
16:00	SOCIAL NETWORKING SPECIAL OPS: EXTENDING DATA VISUALIZATION TOOLS FOR FASTER PWNAGE The Suggmeister	YOU SPENT ALL THAT MONEY AND YOU STILL GOT OWNED... Joseph McCray	SNIPER FORENSICS - ONE SHOT, ONE KILL Christopher E. Pogue	EXPLOITSPOTTING: LOCATING VULNERABILITIES OUT OF VENDOR PATCHES AUTOMATICALLY Jeongwook Oh	GAMING IN THE GLASS SAFE - GAMES, DRM AND PRIVACY Ferdinand Schober,
17:00	GETTING SOCIAL WITH THE SMART GRID Justin Morehouse, Tony Flick	SHODAN FOR PENETRATION TESTERS Michael Schearer	OBOX ANALYZER: AFTERDARK RUNTIME FORENSICS FOR AUTOMATED MALWARE ANALYSIS AND CLUSTERING Wayne Huang, Jeremy Chiu	FUNCTION HOOKING FOR MAC OSX AND LINUX Joe Damato	SECURING MMOS: A SECURITY PROFESSIONAL'S VIEW FROM THE INSIDE metr0

SKYBOXES

	205	206	207-208	209-210	211-212
Thursday					Hacker Karaoke 21:00
Friday	Forum Meet 20:00-02:00	303/SkyTalks Spiders are fun PM	Hackerpimps	Hardware Hacking Village Queercon at 22:00	Lockpick Village
Saturday		303/Skytalks	I-Hacked.com	Hardware Hacking Village	Lockpick Village Hacker Karaoke at 21:00
Sunday		303/Skytalks	HAM Radio Testing in 207	Hardware Hacking Village	Lockpick Village



DEF CON 18 could not have happened without the support of the community! While we don't do this for a pat on the back I still want to personally thank all of you who have helped support DEF CON This year, from passing along information tweets, helping give someone a ride to con, answering questions from a n0Ob, to throwing a party or contest.

I always feel guilty after writing the thank yous and sending them off to be printed because I inevitably remember another person who was overlooked or taken for granted. This is the current working draft. It is tradition to go to the https://forum.defcon.org/ after con and post your own personal stories and thank yous, a sort of crowd source of win! for outstanding con contributions and stories.

I would like to thank: DEF CON Employee #1 Neil, Jeff McNamara, Janet, Zac, Lock, Noid, Kingpin, Nikita, Major Mal, Heather, Doolittle, Videoman, TW, Flea, PyrO, Russ, Ax, Nico, Heather Blanchard, Q, Roamer, Grifter, Rich M, ETA, Ira, BB, Jim Christy, CJ, l3d, Riv management and terrific Theresa. New guys stepping up Wad, Dodger, DJ Great Scott!, All the DJs and live bands! You guys rock! To TOOOL, Ninjas, Hacker Pimps, Delchi, and everyone else throwing a party or adding spice to life. The Forums ninja squad, CotMan, Chris, Thorn, Neil, Alx Rogan, astcell. To THE SPEAKERS! Without you DEF CON would be just (a very cool) party. You guys are the core of the con, and I thank you for all your hard work pushing the boundaries and inspiring others to follow in your footsteps.

Zac Thanks: Lock, Heather, Noid, Flea, Agent X, Proctor, Tw, Tyler, Q, Sunsh1ne, Russ, Pyro, Roamer, Alx Rogan, Major, Alien, Nico, Nicole, Ed, Charel, Theresa, Doug, Dolittle, Mel, Cal, Dodger, Neil, Aaron & Jonathan, and everyone else who works their arse off every year to pull DEF CON off. I'm Proud of you. It gets better every time.

Russr Thanks: hazmat, PyrO, libero, roamer, securitytribe, LosTboy, DT, blackbeetle, wiseacre, Phorkus, the HHV volunteers, and all the other goons, volunteers, and attendees that make this con kick so much ass.

Info Booth Thanks: FAWCR, Melloman, Flwrchld, Jenn, Medic, Dara, ACRONYM, Sweep, Puck, for without them none of this works.

Roamer Thanks: AlxRogan, Evil, Latenite, Redbeard and Wad. Neil, Nikita, and Charel for all of their help coordinating. Theresa from the Riv for her amazing level of support. Godminusone for impromptu guitar lessons. TheCotMan for being the best Forum admin ever and wiseacre for his years of work as a Vendor Goon and his continued behind the scenes support.

Schwag Booth Thanks: Q, SunSh1ne, Fox, Influx McGee, Veruus, Sharon & the folks from Blaine

Speaker Control Thanks: Pwcrack, Goekesmi, Volty, Dallas, Zendog, Pardus, Nevada Raven Whisky Romeo Crash, A-Monkey, Bushy, Code24, #2, Agent X

Security Thanks: Amber, Arclight, Captain, Chosen1, CHS, Eddy Current, Cyber, Cymike, Danozano, DcOde, Flea, Fox Captain, Gadsden, Godminusone, Jdoll, JustaBill, Kallahar, Kevine, Krassi, Kruger, Lei, Londo, Lunaslide, Marygrrl, Mattrix, MAXIMUS, Montell, Nobody, noid, Nynex, P33v3, Pappy, Pescador, Polish Dave, Pool Boy, Priest, Queeg, Quiet, Rik, SkyDog, Tacitus, VectOrx, Vidiot, Whiteb0rd, Xinc, Converge, Angie

Network Thanks: Lockheed, effffn, Heather, Mac, Videoman, Enki, Sparky, Mac, KidKaos, and DJ t3ase!

Nikita Thanks: The Dark Tangent, Neil, Lockheed, & especially all the speakers. Fairies & #pantslesstottenkoph.

Dispatch Thanks: Benson, Chuck, Doolittle, n0ise, Rf, and Voltage Spike, for continuing to hack the Def Con Airwaves!

Music Thanks: All the performers, Mobius, Shadowvex+VJ crew, Zebbler, Kate, Lockheed+NOC, Zziks, Krisz Klink, ChrisAM, Aricon, JoeKV, Cr1stina, Charel, Nikita, Neil, and DT

Skyboxes Thanks: Grifter and l3d for keeping the Skyboxes full of content that feeds your brain while the sun is up, and full of parties that kill your liver when the sun goes down.

Registration Thanks: TW, Cstone, 6q, Crackerjack, & Tyler.

QM Stores Thanks: Major Malfunction, Alien, Dodger, RijeIV, ETA, English Breakfast Tea, Cucumber Sandwiches, and our faithful Wookiee truck driver, Uncle IRA.

-The Dark Tangent, DEF CON 18 eot.