DEFCON
16

welcome to DEFCON 16

Welcome to DEF CON 16!

It has been a long and interesting year in the world of hackerdom, and I am glad to present you all with the latest installment of the unstoppable force that is DEF CON! We have more talks, more contests, more double ++ goodness lined up than ever before!

Ian Angell was cool enough to come over from after giving the day one Keynote at Black Hat to speak here as well. He just can't get enough of Vegas it seems.

What's in store this year? AgentX from speaker control said his crew could handle as many speakers as I could select, so we've got five tracks this year along with post speech Q&A rooms. Take that! We have a new chill out area, where the B&W Ball is to be held at night, and it offers drinks, DJs and wifi, a haven to drop in and chill out when you need to get away from it all. New skybox villages for hardware hacking, wifi and lock picking goodness. Go upstairs to learn some new skills or go to the contest area to flex them.

In the evening we will be screening a new hacker documentary, hosting live bands at the B&W Ball and getting some last drinks at Quarks Bar before it closes this year. Take pictures and post them to pics.defcon.org, talk about the talks you enjoyed on forum.defcon.org, and jump on the (NEW) defcon-16 twitter feed to see what is going on during the con. Remember, the con is what you make of it. We provide the platform, you guys provide the content!

As I write this I am on the roller coaster of con planning. Yesterday Kingpin said some suppliers might not produce the materials in time for the badges to manufactured, despite us starting planning them almost 18 weeks ago.

Stress. Today it looks like they might make it so if you have a badge around your neck then everything turned out ok. Oh! I almost forgot! There are some Easter eggs in some of the con materials, solve them and you will find the path to the bonus round.

Enjoy,
The Dark Tangent

contents

Badge Care & Feeding....2
Blackout Parties....3
Chillout Room....3
Movie Night with DT....4
Contests....6-7
Events....8-9
Outdoor Demos....10
EFF Fundraiser...11
Defcon Swag hours...11
12...Art Contest Winners
13-25...Presentations
26...Defcon Network
27...Vendors
27...Book Signings
28-30...Talk Schedule
30...Skybox Schedule
31...Convention Map
32...Shout outs

the dc16 badge

CARE AND FEEDING GUIDE

If your badge did not come with an SD card slot, a limited number will be available from the Hardware Hacking Village for soldering on to your badge if you would like to take advantage of the file transfer capabilities of the badge.

blackout parties

BLACK AND WHITE BALL IS NOW "THE BLACKOUT PARTIES"

Be sure to bring Glow sticks, Lightsabers and anything else that glows blinks or lights up. (bring a few extras to share)

Dresscode: Glow in the dark, body paint, neon colors, all white or all black.

NIGHT 1 (FRIDAY)
Dark industrial with a twist

3vil_1	industrial goth	20:00	myspace.com/3vil1
Probable Cause Mutated Disco	80's /Electroclash	21:00	myspace.com/metanoise
Regenerator	industrial	22:00	Regenerator.net
Rustcycle	guitar driven electronica	24:00	rustcycle.com
Synnack	industrial	1:00	Synnack.com
DJ Spekulum	Industrial goth	2:00	
Doors Closed	END Friday Ball	3:00	

NIGHT 2 (SATURDAY) IN 101/102
Breaks Beats and Nintendo rock

Minibosses	nintendo rock	20:00	minibosses.com
Mitch Mitchem	breaks electro	21:00	I haveagiantdick.com
great scott!	breaks electro	22:00	djgreatscott.com
DJ Jackalope	Jungle	23:00	dj-jackalope.com
DJ Shem	psytrance	24:00	myspace.com/shem
dangerous phenomena	dirty electro/progressive	1:00	dangerousphenomena.com
krisz klink	psytrance	2:00	

Both nights start promptly at 8pm, and will run unitll 3am.

* lineup subject to change without notice.*

Zziks.

The Blackout Parties are located in the Chillout Room (101/102)

chillout

need a quick place to meet up before the next talk? or a place to launch your next wave of attacks?

stop by the Chillout room

Plenty of room for you and all of your cronies to meet up / discuss / or just hang out.

Open from 12:00 till 18:00 in 101/102

Live Music Provided by Nu Skool Breaks! (NSBradio.co.uk)
- NSB just won "best radio station" for the 2008 Breakspoll (International Breakbeat) awards (http://breakspoll.com) they will be streaming live from the chill room check them out at: NSBradio.co.uk

Scheduled to appear:

Great Scott
Simo Sleevin'
Lazy Boy
Simon Plexus
Phylo
The Scritch
DJ BTZ
Alpina
DJ E-Roc
Vegas breaks

A few words from DJ Miss Jackalope

What? You again? You weren't scared away the first 6 times you came here? I hope you brought some friends to let us teach things to. Aren't you the person who left the first year you were here thinking, "Who were all those strange people and why did they know so much random stuff?"

This year you brought your mom, your boss, your roommate, and your girlfriend's pet tarantula. Well ok, the boss was overkill, and you really should have convinced your girlfriend to come too, only if to see you on Saturday night with 40oz beers duct taped to both your hands and one taped to your crotch, but she had other plans like to go to her Suicide Girl's photo shoot so she could convince more people her last name ended in .jpg.

You were hoping to just have a chill weekend with some friends, but it's only once you've bailed your boss out of jail after doing crazy things during my DJ set at the Ball on Saturday night, and rescued the tarantula from getting eaten on a bet, and saved your roommate from getting whipped by Vinyl Vana at Jeopardy that maybe, finally, you will have a moment to hang out with them...

This was, of course, after you have survived the Toxic BBQ, pounded free cold ones at the Beverage Cooling Contraption contest, tried to force your way into one of LosT's Mystery Boxes, escaped from a Mexican jail cell, got fired upon by robots, attempted to decimate Roamer at Guitar Hero, answered some questions from Winn Schwartau, watched a movie made by his daughter, spotted some Feds, and did some serious phreaking along the way, found some stuff because a list told you to, all while trying to capture a mysterious flag. Did I mention this is only by Saturday? You have a whole other 24 hours to survive after this.

Plan your time well. Make new friends. Trust that your mom can handle herself. (I mean, you came in to the world ok, right?) Don't get in any fights with Ninjas. Learn everything you can. Ask questions. Use a condom. Have a good time. Clean up your mess. Don't get arrested. Come back again.

Your Defcon16 weekend was and will be assessed by Miss DJ Jackalope, DefCon Resident DJ and CD seller. See dj-jackalope.com for further assessments.

movie night

Movie Night with the Dark Tangent
Fri: 21:00, Sat: 19:00 in Speaker Track 1

This year on Friday night we will be screening a documentary, "Hackers Are People Too", which will end before the director/producer needs to participate in Hacker Jeopardy. Then we will move on to some Blu-Ray goodness of "Appleseed Ex-Machina" for the latest in cg anime from Japan.

Saturday evening we will go retro with a 25th anniversary screening of WarGames, Followed by a fireside chat with David Scott Lewis, IT & green tech entrepreneur, model for David Lightman (Wired magazine, August 2008).

Saturday, 19:00, Royale Pavilion 1 & 2
25th Anniversary Showing of Wargames
Followed by a fireside chat with David Scott Lewis, IT & green tech entrepreneur, model for David Lightman

"Hacking was easy back then. There were few if any security measures. It was mostly hackers versus auditing types. The Computer Security Institute comes to mind. I would read all of their materials and could easily find ways around their countermeasures. The part in the movie showing David Lightman perusing the library to find Falken's backdoor password, "Joshua," is clearly a reference to many of my antics.

In those days, there were no blackhats or whitehats. I didn't do anything too serious. Just wanted to see what I could get away with. Just like in the movie."

-David Scott Lewis
(as quoted in Wired magazine, August 2008)

Based in China and affiliated with Tsinghua University (China's MIT), Lewis has held executive positions with Microsoft, Oracle, Samsung and the META Group (now owned by Gartner).

Then we'll close with "Three Days of the Condor", where you can see an early Robert Redford deal with spies, telephones, and intrigue. For those who have seen 'safehouse' you'll recognize a scene for scene rip off homage to "Condor".

contests

NEW CONTESTS FOR DEFCON 16:

Buzzword Survivor
10:00 Fri - 22:00 Sat

10 people listening to 36 straight hours of vendor pitches. Sucks to be them. Winners take home their share of $10K prize

Gringo Warrior
Saturday 11:00-18:00 in the Contest Area

"What happens when a good time goes bad? Imagine the following scenario... you are attending a con in Southern California. On a whim (or possibly at the suggestion of Dan Kaminsky) some folks decide to cross the border into Tijuana for a cheap tequila drink-a-thon. You accompany them, but the evening gets way out of control. You awaken in a small room in the back of what appears to be a run-down police station. You become vaguely aware of uniformed individuals speaking to you in a threatening manner. Making references to violation of laws against public drunkenness, your captors describe monumental fines and penalties. They imply that unless you clean out your bank account using your ATM card unless you will face considerable jail time. They slam the door, saying that they're going to give you some time alone to think about their offer. Your mind races, your brow sweats. Is this really happening? If you comply, what's to stop them from just dumping you in the desert somewhere? Are these people even really police officers? You come to the determination that you have no intention of going along quietly with their plans. Your captors may have confiscated your wallet and passport... but they didn't notice the lockpicks that you were carrying. Participants in Gringo Warrior will have five minutes to free themselves from handcuffs, escape from their ""cell"", get past a guard, retrieve their passport from a locked filing cabinet, leave through another locked door, and make their escape to freedom. 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. The best warrior of all wins the grand prize!"

L337 Ski115

Talent Competition
Sat: 20:00 in Speaker Track 4

A talent show to allow attendees to showcase their "Leet Skills" and show off a hidden talent. We expect to limit acts to approximately 5 minutes in duration and expect the whole talent show to last approximately 60 minutes, or 1 hour."

MSK Security Challenge
Fri & Sat: 10:00 - 20:00
Sun: 10:00 - 14:30p

$500 prize for anyone who can log into a website or hack the shopping cart that is secured by MSK Security. The first person to retrieve a secret password will receive the $500 cash prize

The Race to Zero
Friday 10:00 - 18:00 in the Contest Area

The Race to Zero involves contestants being given a sample set of viruses and malcode to modify and upload through the contest portal. The portal passes the modified samples through a number of antivirus engines and determines if the sample is a known threat. The first team or individual to pass their sample past all antivirus engines undetected wins that round. Each round increases in complexity as the contest progresses.

Returning Favorites

Badge Hacking Contest
All Con until 14:00 Sun

The DEFCON Badge Hacking Contest exists to award the top 3 most ingenious, obscure, mischievous, obscene, or technologically astounding badge modifications created over the weekend."

RETURNING CONTESTS:

Beverage Cooling Contraption Contest (BCCC)
Fri 12:00 in the Contest Area

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? Teams will put their wits and their fabrication skills to the test in the hope of developing technological contraptions that can accept liquid input (which may range between 70º or over 90º, depending on the Las Vegas sun) and cool said beverage to below 40º in as little time as possible. With bonus points being awarded for cost-efficient, energy-efficient designs as well as creative aesthetic choices, even bystanders are likely to get a kick out of the proceedings. Heh… and if that's not enough encouragement for you, bear in mind that there will be plenty of free beverages available for participants to, ahem, "calibrate their equipment" and so forth. That often leads to an excess of technology output and we have to do something with it… so drop on by and have a good time with us!

Capture the Flag
All Con until 14:00 Sun

The following teams have demonstrated their uber prowess by qualifying to participate in the DEFCON 16 Capture the Flag Contest, organized by Kenshoto.

These 7 teams will be battling last year's winners, 1@stPlace, for the CTF title! DEFCON would like to congratulate all of these talented teams and wish them luck!

Routards
Pandas with Gambas
Guard@MyLan0
Shellphish
Taekwon-V
WOWHACKER
PLUS

Clued
Thu 12:00 - Sat 18:00

Information is everywhere. Solve the puzzles, solve the mystery.

The Official DefCon CoffeeWars

Friday @ 10:00 in the Contest Area

"Bring your best beans and put 'em up for judgment by our over-qualified, over-caffeinated, (and over-rated) Coffee Wars judges and contestant panel! We keep hearing that someone else's beans are the best. Now it's time to prove it bean-to-bean!"

DEFCON bots
Computer Controlled Weapons Development

Practice Friday 24th
Contest Saturday - 13:00

The DefconBots contest pits two fully autonomous robotic guns against each other in a challenge to see who can shoot down the most targets in a shooting gallery the fastest.

Guitar Hero (GH3 Madness & DC16)
Fri / Sat in the Contest Area

Another year, another Guitar Hero contest! Remember that big tournament held every March in cities across the US? That's right! Guitar Hero 3 will be straight up tourney style…single elimination, entirely heads up. Move up the brackets against multiple opponents to eventually be crowned the newest Defcon Guitar Hero! Stop by the GH3 table Friday morning from 10am to noon to sign up. The tournament will start at 1pm Friday afternoon and extend into Saturday. All information can be found at the contest table in the contest area, including the most up to date schedule, standings and times.

Hacker Jeopardy
Fri 21:00 - 23:00, Sat 21:00 - 23:00 in Speaker Track 4

Hacker Jeopardy: Is on again this year!Check it out starting at 21:00 in speaking track 4 Friday and Saturday Night! Finale starts at midnight Saturday!

LosT @ Con Mystery Challenge
All Con until 14:00 Sun

The Mystery Challenge is just that- a mystery. Each year teams sign up for a challenge whose details are not revealed until the first day of Defcon. Past Mystery Challenges have required skills in cryptography, mathematics, lockpicking, network protocols, RFID hacks, social engineering, electronics, riddle/puzzle cracking, phreaking and hardware hacking. Mystery Challenge embodies the true spirit of the hacker, as it requires teams to work together to overcome obstacles and observe hints and information often hidden in plain sight.

Website:
www.mysterychallenge.org

oCTF (Open Capture the Flag)
Fri 10:00 - 22:00
Sat 10:00 - 22:00

Formerly known as Amateur Capture The Flag (aCTF), this contest pits any Defcon attendee against the house (DC949) as well as other contestants. There are a series of challenges of varying difficulty involving a variety of things, including cryptology, steganography, malicious software, and websites (and other services) just waiting to be exploited.

Last year, DC949 reminded all the contestants why they shouldn't install software from untrusted sources; this year we expect more lessons will be learned the hard way. Is your software safe? What about your hardware?

This contest is open to everyone, including novice hackers, and is designed to challenge a range of skills and provoke logical thinking. Each team will get one ethernet port (and we'll do our best to provide as much cat5 as we can afford). Donations are accepted (paypal icon on the right). It'll take place Friday and Sat from 10:00 - 22:00 (subject to change) in the contest room. Registration is not strictly required, but it'll help us plan things, and those who register will be rewarded.

Own the Box @ DC16: Pwning for dollars
Times TBD in the Contest Area

Own The Box, now in year 0x01, continues its hallowed tradition of creating temporary autonomous zones of random people asking to be haxored. We're a defender contest, of sorts, which means the following:

Contestants bring a server, running some hardened services
We invite all DefCon attendees to attack these services
????
PROFIT

This year, we made some changes to the format: Instead of asking defenders to offer up their hardware to successful attackers, we're glomming on to the Vegas spirit and making this a contest of cold, hard cash.

Defenders pay a nominal entry fee, matched by contest organizers, the Cosa Nostra, and Dan Kaminsky's grandma. The winning entry, based on services uptime and our patented PwnOMeter(tm), gets the cash, as a tab at the Splash bar, on Sunday afternoon.

We're also partnered up with the good folks of OCTF, so entries will be targets in their contest, and given varying point levels in OCTF throughout con, guaranteeing a dedicated pool of attackers to bring the love."

the phreaking challenge
Fri: 11:00 - 17:00
Sat: 13:00 - 17:00
Sun: 13:00 - 14:30

Announcing the less new, but much improved Phreaking Challenge! Prepare to test your skillz in old skool and new-school telephony arts. The challenge will include traditional TDM-style phreaking skills as well as ""VoIP/Converged"" tasks. Players will prove themselves at DTMF recognition, phone closet land navigation, general telecom knowledge, and newer technologies. This culminates in a final round that combines all these talents with a touch of classic detective work a la the Dumpster Dive."

TCP/IP Drinking Game
20:00 in Speaker Track 4

The annual must-see Defcon event of BGP, booze, and bemusement returns in this year's TCP/IP Drinking Game. Panelists will pit their trivial knowledge of network trivia against one another and the ever-present haze of inebriation for all to see. We promise that no RFC nor hepatic system will be spared. As always, solid audience participation is encouraged, so bring well-researched queries.*

This year's event will be hosted by Adam J. O'Donnell, security researcher and provocateur.

The usual M.C. of the TCP/IP drinking game, Dr.Mudge, is spending this year sober for tax purposes... see you next year with my new bionic liver :)

.mudge

* Anyone asking about Windows 98 TCP/IP UIs will be promptly ejected.

Scavenger Hunt
12:00 - 19:00 Friday
12:00 - 18:00 Saturday
In the Contest Area

Wall of Sheep
All the time

Lockpick Contests
Various times

Points Competition

You've seen this one before... a large number of the public locks in the village are specially marked as part of this challenge. DefCon Attendees who hang out in the village can present opened locks to the staff who will record their achievement on a master score sheet which shows a running total. The individuals with the highest scores by Sunday at noon (or the individual(s) to open every point-valued lock the soonest) are awarded some swag and other prizes that we can wrangle.

Lock Field Stripping

This contest was a hit last year (it was a wonderful on the spot creation by Schuyler) and it will be happening again. Contestants will be given a simple lock core and tasked with fully breaking it down to its component parts. That means (in addition to getting it unlocked and opened without a key) they will have to pull the plug, eject all the pins and springs, and keep these parts in relative order... because with that checkpoint cleared, they must re-assemble the lock in such a way that the original key still functions. We promise to have an announcement for when this will take place by Friday at noon, if not before.

Speed Picking Competition

This will be a test of skill in the vein of what has been historically called the LPCon... you've seen it with KaiGoth, DC719, Doc, and the rest of the wonderful people who've hauled tons of gear with them to Vegas every year. Simple, straightforward, timed picking is the name of the game here. No special tools, snap guns, bump keys, etc... just you and your thin bits of steel. This year the contest will be officially called the "American Open" as it will follow the rules set forth by the European competitions such as the Dutch Open. Players will be reduced in heats and rounds via head-to-head face-offs in which two locks are opened, then swapped, then opened again (to eliminate any chance of uneven lock difficulty) etc etc. This will separate the men from the boys, the ladies from the lasses, and the leeto burritos from the nooby nachos.

Reflections on the Mystery Challenge

I get asked to explain the Mystery Challenges quite frequently. More frequently than that I am asked what the hell it is in the first place. I find it interesting that nobody ever asks why the Mystery Challenge (which has really come to be called 'Mystery Box'). Why I spend months of my life, thousands of dollars and all my time at Defcon creating ciphers that are meant to be broken, strong boxes that are supposed to be breached, and circuits that are designed to be destroyed.

The truth is I created the Mystery Challenge with one thought in mind- to create a contest that I would want to compete in myself. The problems I have to overcome in the Mystery Challenge designs are my personal bout with myself. Every year I compete in a contest that has only one player. It is an 'inner tournament' that I have created. The actual event that takes place at Defcon is simply a by-product of this private solo challenge. Success in designing a good Mystery Challenge brings a sense of accomplishment that I doubt I could find any other way. I was amazed when Defcon 15's Mystery Challenge brought with it a tangible reward in the form of a coveted Black Badge. I had actually been awarded a Black Badge for winning a mental contest I had created for myself. It felt like the ultimate hack.

So what is the contest you ask? It's a mystery. Teams never know what challenges they will face each year. In the past there have been elements of: mathematics, cryptography, stego, languages, pirate maps, circuit schematics, electronics prototyping, social engineering, lockpicking, riddle solving, powers of observation, RFID, telephony, optical encoding, bomb diffusing, metal work, coding, number base conversions, binary palindromes, one time pads, Fibonacci sequences, the letter "e", neodymium magnets, and the Venture Brothers' robots, to name a few. For me personally nothing will ever top the first year, when I actually gave the teams the solution, right in the beginning; it was there in front of them the whole way! I often wonder how many answers to other problems we already have, and just don't realize it. -LostboY, Defcon 16

events

DEFCON Shoot

The DEFCON Shoot is a public event happening just prior to the DEFCON hacker conference in Las Vegas, Nevada. Anyone who wants to can show up and for a small fee make use of a private range located about 30 minutes outside of the city. There will be opportunities to see and possibly shoot some of the weapons belonging to your friends and it will also be possible to rent firearms (including Class-III full autos) from the range itself. In addition to having a number of terrific pieces of hardware on-site, the range is directly affiliated with Small Arms Review Magazine and thus has access to their nearly limitless archive of equipment. Anything from a WWII Bren Gun to a Vulcan Cannon-style Minigun is possible.

This year's DEFCON Shoot will take place on the morning of Thursday the 7th. We hope to begin rallying all interested parties in the lobby of the Riviera Hotel around 6:00 and be underway by 6:30. The shoot itself will take place approximately from 7:00 AM to 10:00 AM at Desert Lake Range.

Toxic BBQ

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

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

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

See toxicbbq.com for details

Titanium Chef @ the Toxic BBQ

So... do you fancy yourself to be a skilled person around the kitchen? Do your friends all rave about how great your cooking is no matter what's being served? Well, there's the possibility that you're attractive and they're just trying to use praise as a way to get into your pants, but if you truly possess culinary skill perhaps you have what it takes to participate in a new event that will take place at this year's ToxicBBQ... the Titanium Chef Challenge.

Much like the popular televised Japanese program "Iron Chef", this competition will involve the speedy preparation of dishes using a theme ingredient to be revealed shortly before the ToxicBBQ begins.

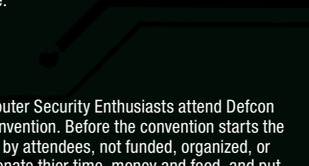
theSummit

Thu: 21:00 At the Top of the Riv

theSummit is a fund raiser for the EFF, a nonprofit group of passionate people - lawyers, technologists, volunteers, and visionaries - working to protect your digital rights.

In addition Vegas 2.0 has added The Hacker Foundation to theSummit's benefactor list! All procceds will be split between the EFF and The Hacker Foundation!

Details:
Location: Top of the Riv (top floor of Monaco Tower)
Thursday Aug 7, 2008
9:00PM - ???
Tickets $40 @ door
All Ages Event!



Performers:
Dual Core and The Brothers Grim will be performing at this event.

Queercon

Fri: Mixer 16:00 in DJ/Chillout, Club Queercon 20:00 in Skybox 211

Hey GLBT hackers; Queercon is on for its 5th year at Defcon! If you're gay/lesbian or just friendly, come meet others like you among the hacker community. We're here, we're queer, everyone's already used to it, so let's drink! To that end, Queercon is two seperate events again this year. First up is the Queercon mixer, Friday at 4pm at DJ Chillout area in 101/102 Come drink, socialize, make plans, swap stories. Then the main event is Club Queercon, Friday at 10pm in skybox 211. We have several DJs lined up, glowsticks, and hopefully a staffed bar at your disposal. All are welcome, if friendly. The first few proud hackers at the mixer will get a free drink for the Club! Hope to see you there.

DEFCON Forum Meet

Fri: 20:30 in Q&A 5 (Room 103)

The Forum Meet is a way for members of our online community to get together and hangout in person. It also gives us a chance to catch up on all the ins and outs that have happened since last year, share awesome goodies, wii codes, and act as though we just saw each other a week ago. This years Forums Meet is brought to you by: Converge, Lil_freak, Meee, DaKahuna, & Mixitup.

What: The Official Defcon Forum Meet
When: Friday August 08, 2008 from 20:30hrs to 22:30hrs.
Where: Q&A Room 5 (Room 103)
Why: So we can get together and meet.

QUANTUM SPOOKSHOW

Fri & Sat: 10:00-19:00, Sun: 10:00-16:00 in the NIST Quantum Crypto Lounge (Room 114)

Quantum mechanics make possible some things that are impossible in the "classical" world of ordinary experience, and which even seem to contradict common sense. Some of these spooky effects are coming into practical use in security applications. The Quantum Spookshow of the National Institute of Standards and Technology (NIST) and the National University of Singapore (NUS) demonstrates quantum cryptography and quantum entanglement on a four-node quantum network, which supports quantum encrypted streaming video and violations of local realism. Participants are encouraged to interact with the light beams that constitute the physical link of this network, and to meet physicists who have designed and built quantum networks. Quantum mechanics provides methods of encryption that are secure from eavesdropping attacks against the quantum channel, but in any actual system there are points of vulnerability, e.g. correlations of classical noise in the operation of quantum elements. Participants will have a chance to discover vulnerabilities by hands-on interaction with our systems.

This demo to run 10:00 to 19:00 on Friday and Saturday, 10:00 - 16:00 on Sunday, in 114 located directly across from the Contest Area. For further information, see http://havephotonswilltravel.com

WORKSHOPS

EEEPC Mod Workshop Meetup

Sat 13:00 - 15:00 in the Contest Area

This is more of a LUG for EEEPC users than a true workshop. If you have an EEE with you that is modded in some way or fashion either via software (what do you mean it runs OSX?!) or hardware (it turns your house lights on with Bluetooth and waxes your cat?), please bring it by! We will be there to share ideas, advice, and other crazy EEE things. The main purpose of this event is to give ASUS EEE PC owers an opportunity to show and tell others about any useful hacks they have discovered or created that add feature, functionality or deadliness to the EEE PC"

DAVIX Visualization Workshop

Sun 14:00 in Speaker Track 5

Need help understanding your gigabytes of application logs or network captures? Your OS performance metrics do not make sense? Then DAVIX, the live CD for visualizing IT data, is your answer!

To simplify the analysis of vast amounts of security data, visualization is slowly penetrating the security community. There are many free tools available for analysis and visualization of data. To simplify the use of these tools, the open source project DAVIX was put to life and is released this year at BlackHat/DEFCON.

At this "Bring Your Own Laptop" workshop we will introduce you to DAVIX. The workshop starts with an introduction to the set of available tools, the integrated manual, as well as customizing the CD to your needs. In a second part, you can use DAVIX to analyze a set of provided packet captures. In the end we will show some of the visualizations created by the participants. Be prepared for pretty and meaningful pictures!
For you to be able to participate in the analysis part of the workshop, you should bring an Intel or AMD x86 based notebook with at least 1GB of memory and a wireless LAN adapter. To avoid problems with the Wireless card setup we strongly recommend that you run DAVIX in VMware Player or VMware Fusion in NAT mode. The DAVIX ISO image should be downloaded before the workshop from the davix.secviz.org homepage. The network capture files will be made available during the workshop.

VILLAGES

Hardware Hacking Village

Fri & Sat: 10:00-20:00, Sun: 10:00-14:30 in skybox 209

Welcome to the new Hardware Hacking Village, located in Skybox 209, upstairs from the contest area. The HHV examines the hardware and software aspects of embedded systems. Have you always been interested in the hardware side but didn't want to embarrass yourself in front of your peers? Are you confused about the difference between and resistor and a capacitor? Ever wonder how that remote control works? Do you constantly get sand kicked in your face at the beach? Now is your chance to learn the basics and get started. The Hardware Hacking Village will be offering presentations, tutorials, an guidance throughout the conference for attendees interested in learning the basics, or asking questions on more advanced topics.

The HHV will be selling a limited number of custom Defcon branded micro-controller kits (available in the vendor area), and will also be home to the Defcon Badge Hacking contest. Two kits will be available for purchase and use during the presentations and other mad scientist experiments. The primary kit includes the micro-controller parts, which can be assembled in the HHV alone or with guidance from knowledge volunteers. The expansion kit includes a servo and a number of other parts for use in your dastardly plans for world domination. Whether you use these kits to just learn the basics, or you use them to give yourself a leg up in the badge hacking contest, you'll never find a better price on a truly cool, limited edition kit of this kind!

Lockpicking 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.

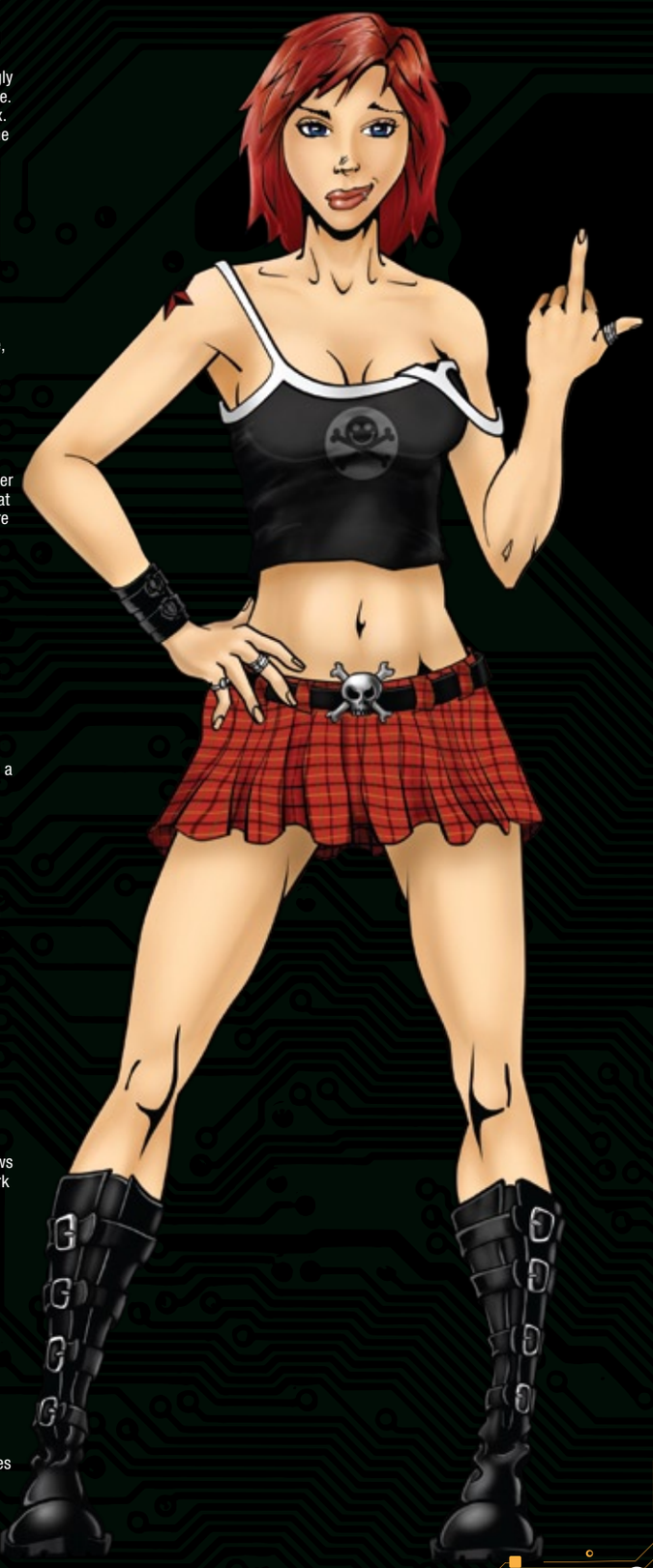
The Lockpick Village is a demonstration and participation area on the skybox level at DEFCON. In this workshop environment attendees can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice with locks of various levels of difficultly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

Wireless Village

Fri-Sun Skybox 210

The Church of WiFi excitedly presents the Defcon 16 Wireless Village. Topics could include but have no limitation: 802.11x, 802.16, Bluetooth, IR, CDMA, GPRS, Amateur Radio... think it, do it! The sub-con will be home of amazingly super-krad breakouts, demos, contests, and the finest invisible hand-on activities folks can dream up between now and August. http://www.churchofwifi.org . Located in Skybox 210 Friday through Sunday



outdoor demos

Mobile Hacker Spaces

Interested in visiting a Colorado Hacker Space here at DefCon 16? Check out the first ever Mobile Hacker Space, which will be parked in the outside chill out area during the convention. Try your hand against one of the challenges in the pentest lab, or learn from the web-based tutorials posted on the open network. Participation is encouraged, and presentations will be given every day from 2-4pm, which will provide a more hands-on look at how the Mobile Hacker Space operates and fits within published hacker space design patterns. Make sure you also attend the presentation on the history and design of the Colorado Springs Mobile Hacking Space on Sunday, at 1pm in Track One.

Fri, Sat, Sun 14:00-16:00pm
Outdoor Area

WarBallooning Demo - "Kismet Eye in the Sky"

Introduction
A WarBalloon, er... Airborne Surveillance & 802.11 Stumbling Platform, also know as the "Kismet Eye in the Sky" will be flying just outside the DECON convention center on FRI and SAT from 11AM - 2 PM. DEFCON Attendees: please note the Balloon & Electronics launch will occur Daily at 11:00 AM & several times during the day as we change antenna's & recon. new targets.

Concept:
Using the balloon to reach a height of ~15 stories, team Tenacity will launch the combo of a Kismet drone (WRT54G), wireless camera (DLINK 5220) & collect data utilizing various high-gain antennas. Kismet Drone collects network data, while the DLINK 5220 camera functions as both a "pan & tilt" mechanism to move the antenna around & simultaneously transmit pictures back to ground. We plan to call in wireless targets from CON members, remotely aiming the eye in the sky antenna from a remote fiber-optic link. Kismet CSV files & video will be distributed to DEFCON members post-CON.

WarDrivers, COWF, and curious all welcome. Drop by & see video of Vegas Strip targets & the giant WarBalloon being piloted over the RIV during DC16.

WHEN:
Fri & Sat 11:00 -13:00 PM Outdoor Area convention center (where dunk tank was located DC15) Hosted by: rocketman & Team Tenacity

eff fundraiser

This year we decided to replace our beloved Dunk Tank with something NEW!

Hackers and Guns in Las Vegas – Ya gotta love it.

You've seen it played out numerous times in movies and on TV. A flash bang grenade goes off. SWAT kicks in the door and moves quickly to differentiate between the good guys and the bad guys in the same room. How do they train to effectively recognize and take out the bad guys, while not wasting any of the hostages? One of the tools they use is a Firearms training Simulator or FATS system and someone was foolish enough to let us get our hands on one for DEFCON 16.

So… Calling all Shooters, FPS Gamers, Psycho Killers, and 1337 wannabes. Come on by and pop a cap in someone's VR ass. We will be set up in room #115 directley across from the contest area. See if you got the skillz to make it through the challenges unscathed. Then the next time you hear a knock at your door in the middle of the night - you'll be ready.

The Skill Drills courseware comprises training drills that focus on the improvement of your student's speed, accuracy, and decision making skills. This courseware was developed by training professionals to focus on hand-eye coordination and has been tested by active Military and Law Enforcement instructors to ensure its training effectiveness. The courseware consists of drills that allow individual combatants to execute training exercises designed to improve target acquisition using laser-based training or Laser Shot's exclusive Live-Fire System Trainer. Each drill allows an instructor to tailor every training session, using adjustable settings such as number of targets, target face time, target speed, and more, for individual skill levels from beginner to expert.

All proceeds go to support the Electronic Frontier Foundation – Leading the fight to protect your personal privacy and digital rights since 1990. More info at EFF.org

defcon swag

Official DEFCON Store Hours

Thu 12:00-22:00
Fri 8:00-22:00

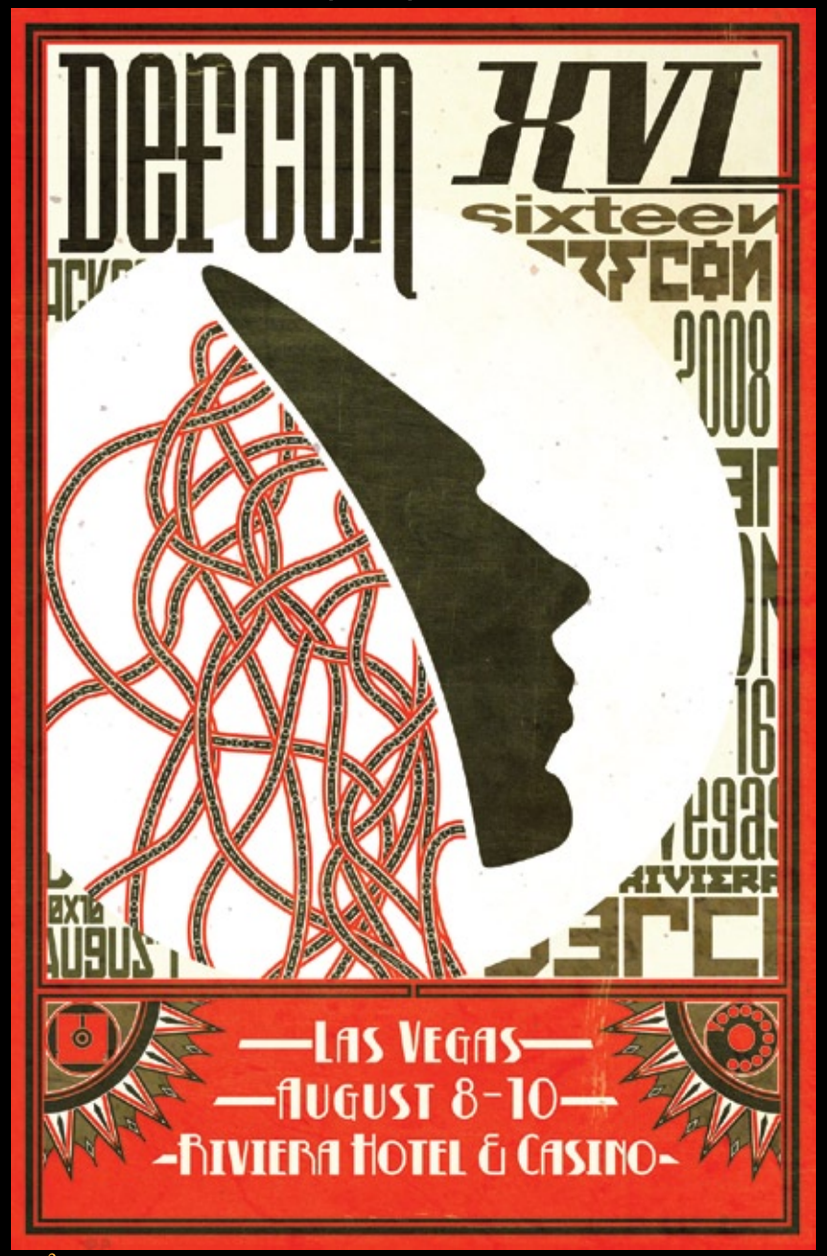
Located at the East Registration desk across from DEFCON registration

Sat - Sun in the Vendor Area at the J!nx Hackwear booth

art contest

CONGRATULATIONS TO ALL OF THE DEFCON 16 ARTWORK CONTEST WINNERS

First Place Winner “Machina” by Astrofy



2nd Place Winner: “Lucha Libre” by Schuyler

3rd Place Winner: “Goons Need Beer” by Deviant Ollam

People’s Choice Winner: “Unsigned Noir” by Gen

presentations

BackTrack Foo - From Bug to Oday

Mati Aharoni
Owner, Offensive Security

As pentesters and hackers we often find the need to create our exploits on the fly. Doing this always presents a challenge. But one challenge took us to a new limit and a new level. We want to share the method with you. From Bug to 0Day will show the audience the process of fuzzing, locating the bug, using egghunters then figuring out to build a pure alphanumeric shellcode to exploit it.

This will truly be the most mind bending 60 mins you will spend in exploit development.

Autoimmunity Disorder in Wireless LAN

Md Sohail Ahmad
Senior Wireless Security Researcher, Airtight Networks Inc.
JVR Murthy
Senior Wireless Security Researcher, Airtight Networks Inc.
Amit Vartak
Senior Wireless Security Researcher, Airtight Networks Inc.

An autoimmune disorder is a condition that occurs when the immune system mistakenly attacks and destroys healthy body tissue. This presentation is about discovery of autoimmunity disorder in select open source and commercial 802.11 AP implementations. By sending specially crafted packets, it is possible to trigger autoimmunity disorder and cause AP to turn hostile against its own clients. Eight examples of autoimmune disorder will be demonstrated.

Autoimmunity disorder can be exploited to craft new DoS attacks. Although 802.11w promises immunity from DoS attacks, we show that autoimmunity disorder leaves a door open through which DoS attacks can still be launched. One example of DoS attack against MFP(11w) will be demonstrated.

Time-Based Blind SQL Injection Using Heavy Queries: A Practical Approach for MS SQL Server, MS Access, Oracle and MySQL Databases and Marathon Tool

Chema Alonso
Microsoft MVP Windows Security,Informática64
José Parada
Microsoft IT Pro Evangelist, Microsoft

This presentation describes how attackers could take advantage of SQL Injection vulnerabilities using time-based blind SQL injection. The goal is to stress the importance of establishing secure development best practices for Web applications and not only to entrust the site security to the perimeter defenses. This article shows exploitation examples for some versions of Microsoft SQL Server, Oracle DB Engine, MySQL and Microsoft Access database engines, nevertheless the presented technique is applicable to any other database product in the market. This work shows a NEW POC Tool.

The Anatomy of a Subway Hack: Breaking Crypto RFIDs and Magstripes of Ticketing Systems

Zack Anderson
Student, MIT
RJ Ryan
Student, MIT
Alessandro Chiesa
Student, MIT

Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.

Digital Security: a Risky Business

Ian O. Angell
Professor of Information Systems. London School of Economics

In this talk Professor Angell will take the devil’s advocate position, warning that computer technology is part of the problem as well as of the solution. The belief system at the core of computerization is positivist and/or statistical, and that itself leads to risk. The mixture of computers and human activity systems spawns bureaucracy and systemic risk, which can throw up singularities that defy any positivist/statistical analysis. Using black humour, Angell discusses the thin line between the utility of computers and the hazard of chaotic feedback, and ends with some advice on how to survive and prosper amongst all this complexity.

VulnCatcher: Fun with Vtrace and Programmatic Debugging

atlas

Countless hours are spent researching vulnerabilities in proprietary and open source software for each bug found. Many indicators of potential vulnerabilities are visible both in the disassembly and debugging, if you know what to look for. How much can be automated? VulnCatcher illustrates the power of programmatic debugging using the VTRACE libraries for cross-platform debugging.

Pen-Testing is Dead, Long Live the Pen Test

Taylor Banks
Security Evangelist
Carric
DEFCON Goon

This talk explores the death and subsequent re-birth of the penetration test. Comprised of conclusions drawn from the collective experiences of two seasoned pen-testers, our talk is filled with facts, fun and rhetoric. We will describe the landscape, the problems, and offer real solutions.

In our talk, we will explore the problems with modern-day pen-tests and pen-testers, and ways to stand out amongst the frauds selling their lackluster vuln-scan services under the guise of a true penetration test.

We discuss penetration tests that are overly tool-driven and/or lacking in methodology as well as pen-testers who lack the experience and creativity to identify the architectural problems that real attackers frequently exploit.

Along the way, we’ll discuss the difficulties faced by real penetration testers and complement these with real-world war-stories to provide both context and comic relief.

Most importantly, we’ll discuss how to solve these problems, through contributions to open methodologies, transparency in process, and shifts in technological paradigms. We’ll tell you how to deal with the latest technologies, even those that change day-by-day. For those that take penetration testing seriously, this talk will be a fun, informative and enlightening presentation on the things we need to do to keep pen-testing worthwhile. Attendees will learn how to perform pentests accurately and obtain compelling and valuable results that ensure real return on investment for their clients.

Owning the Users with The Middler

Jay Beale
Senior Security Consultant and Co-Founder, Intelguardians Network Intelligence, Inc.

This talk introduces a new open source, plugin-extensible attack tool for exploiting web applications that use cleartext HTTP, if only to redirect the user to the HTTPS site. We’ll demonstrate attacks on online banking as well as Gmail, LinkedIn, LiveJournal and Facebook. We’ll also compromise computers and an iPhone by subverting their software installation and update process. We’ll inject Javascript into browser sessions and demonstrate CSRF attacks.

Our new tool, The Middler, automates these attacks to make exploiting every active user on your computer’s network brain-dead easy and scalable. It has an interactive mode, but also has a fire-and-forget mode that can perform these attacks automatically without interaction. Written in Ruby, this tool is easy to both extend and add into other tools.

They’re Hacking Our Clients! Introducing Free Client-side Intrusion Prevention

Jay Beale
Senior Security Consultant and Co-Founder, Intelguardians Network Intelligence, Inc.

In the face of far stronger firewall and IPS-protected perimeters, attackers are compromising far more systems by hacking our web browsers, e-mail clients, and office document tools. Unfortunately, vulnerability assessment practices still focus on checking listening services, even on workstations. Detecting vulnerable clients is left for patch management tools, which aren’t in consistent or wide enough use. Even when organizations are able to invest the time and money in a patch management system, a series of critical problems keeps the botnet builders in business.This talk, by Bastille UNIX creator Jay Beale, introduces a free tool to detect vulnerable clients and keep them out of the botnets.

Predictable RNG in the vulnerable Debian OpenSSL package, the What and the How

Luciano Bello
Engineer (Information Systems), CITEFA/Si6
Maximiliano Bertacchini
Researcher, CITEFA/Si6

Recently, the Debian project announced an OpenSSL package vulnerability which they had been distributing for the last two years. This bug makes the PRNG predictable, affecting the keys generated by openssl and every other system that uses libssl (e.g.. openssh, openvpn). We will talk about this bug, its discovery and publication, its consequences, and exploitation. As well, we will demonstrate some exploitation tools.

When Lawyers Attack! Dealing with the New Rules of Electronic Discovery

John Benson “jur1st”
Electronic Discovery Consultant

The legal community is slowly accepting that the changes to the Federal rules which change the law’s approach to electronic evidence are not going away. Vendors are clamoring to sell their e-discovery “solutions” to law firms and corporations alike, often taking advantage of the uncertainty that comes with such sweeping changes to the law.
The changes to the Federal Rules change the way in which individuals and organizations approach their data much in the same way Sarbanes-Oxley has over the past few years. Instead of merely

creating compliance headaches for security professionals, however, these changes take data security out of the hands of those charged to protect it and spread data to the wind.
More frightening for individuals doing security research is the fact that these rules apply to the one man research operation as the multimillion dollar conglomerate in the same way.

This talk outlines how the electronic discovery process works, why it is costing corporations millions of dollars (but doesn't have to) and will empower attendees with the knowledge they need to deal with this new legal environment.

The Emergence (and Use) of Open Source Warfare

Peter Berghammer
CEO, Copernio Holding Company

The presentation will deal briefly (20 minutes) with the concepts surrounding Open Source Warfare (OSW) and broader adoption for use not only within the context of war fighting, but also its uses within the political arena in order to influence opinion.

The presentation will only deal with publicly available data, couple with real world deployment examples. It WILL NOT contain any type of classified data or anything that can be construed as such.

OSW has become a highly lucrative area that covers topics such as computer security, shaping of potential battlefields and populations, and actual in the field uses of mutated electronics devices such as microwave ovens, model rockets, remote controlled aircraft as well as computer based command and control protocols. What is so particularly interesting in this presentation (as well as the field itself) is how under funded and ill-equipped insurgency (and counter insurgency) groups can make use of off-the-shelf technology to fight against vastly better funded armies. It will also examine communications methods of these groups - and how they approach not only Internet style communication (and in some cases set up their own superior communications networks) but also how they approach communications security.

What To Do When Your Data Winds Up Where It Shouldn't

Don Blumenthal
DMB & Associates

Stories about the loss of sensitive data are becoming more common, and an untold number of others probably are not known because they were not covered by law or did not get the attention of regulators. A loss may happen when data is stolen or simply lost, or when a system is breached. Existing federal and state laws cover specific industries and prescribe particular responses, but pending legislative proposals threaten to expand coverage significantly.
This presentation will discuss the relevant federal and state laws concerning disclosure of sensitive information. In addition, it will explore the elements of a plan for responding to a data loss and the considerations that occur should that plan have to be put into use. These plans, elements, and considerations are critical for addressing a data loss and for dealing with such disparate groups as regulators, the public, employees, and shareholders after your, and their, data is gone.

Working with Law Enforcement

Don M. Blumenthal
DMB & Associates

Security-related laws and regulations, with parallel privacy measures, are assuming an ever-expanding role in American society. As a result, the likelihood that an organization will receive a call, visit, subpoena, or letter from a law enforcement agency is constantly increasing. This program will address issues related to addressing these contacts. It will explore relevant legal questions but also the real world processes and considerations that should go into protecting private sector interests, and even lessening the burden of government inquiries. In addition, it will discuss considerations concerning proactive fostering of relationships with law enforcement to mutual benefit.

Generic, Decentralized, Unstoppable Anonymity: The Phantom Protocol

Magnus Bråding
Security Researcher, Fortego Security

Recent years, and especially this past year, have seen a notable upswing in developments toward anti online privacy around the world, primarily in the form of draconian surveillance and censorship laws (both passed and attempted) and ISPs being pressured into individually acting as both police and informants for commercial interests. Once such first steps are taken, it's of course also of huge concern how these newly created possibilities could be used outside of their originally stated bounds, and what the future of such developments may be.

There are no signs of this trend being broken anytime soon, and combined with the ever growing online migration of everything in general, and privacy sensitive activities in particular (like e.g. voting and all kinds of discussions and other personal groupings), this will in turn unavoidably lead to a huge demand for online anonymization tools and similar privacy means.

If not designed carefully though, such anonymization tools will yet again be easy targets for additional draconian legislation and directed (il)legal pressure from big commercial interests. Thus, a good, robust and theoretically secure design for an anonymization protocol and infrastructure is needed, which is exactly what is set out to be done with this project.

What is presented in this talk is the design of a protocol and complete system for anonymization, intended as a candidate for a free, open, community owned, de facto anonymization standard, vastly improving on existing solutions such as TOR, and having the following important main properties and design goals:

1. Completely decentralized.
2. No critical or weak points to attack or put (il)legal pressure on.
3. Maximum resistance against all kinds of DoS attacks.
   - » Direct technical destructive attacks will practically be the only possible way to even attempt to stop it.
4. Theoretically secure anonymization.
   - » Probabilistic methods (contrary to deterministic methods) must be used in a completely decentralized design like this, where no other peer can be trusted, so focus is put on optimizing these methods.
5. Theoretically secure end-to-end transport encryption.
   - » This is simple in itself, but still important in the context of anonymization.
6. Completely (virtually) isolated from the "normal" Internet.
   - » No one should have to worry about crimes being perpetrated from their own IP address.
7. Maximum protection against identification of protocol usage through traffic analysis.
   - » You never know what the next draconian law might be.
8. Capable of handling larger data volumes, with acceptable throughput.
   - » Most existing anonymization solutions are practically unusable for (or even prohibit) larger data volumes.
9. Generic and well-abstracted design, compatible with all new and existing network enabled software.
   - » Software application developer participation should not be needed, it should be easy to apply the anonymization to both new and already existing products like e.g. web browsers and file transfer software.

The Phantom protocol has been designed to meet all these requirements, and will be presented in this talk.

Buying Time - What is your Data Worth? (A generalized Solution to distributed Brute Force attacks)

Adam Bregenzer
Security Researcher

Brute Force attacks are often marginalized as a user issue or discounted as a non-issue because of sufficient password complexity. Because rainbow tables have provided a re-invigoration of this type of attack, maintaining password security is simply not enough. In this session, I will be releasing a framework for easily creating a brute force attack tool that is both multithreaded and distributed across multiple machines. As computing power continues to grow along with the ability to rent cycles and storage space, it becomes reasonable to add a money-time trade-off to brute force and dictionary attacks. Distributed computing combined with rainbow tables mean brute force attacks can now be very effective. I will present a version of a popular brute force tool which I modified to increase its speed by several orders of magnitude. Additionally I will demonstrate how to adopt an existing tool to utilize this framework.

ModScan: A SCADA MODBUS Network Scanner

Mark Bristow
Security Researcher

ModScan is a new tool designed to map a SCADA MODBUS TCP based network. The tool is written in python for portability and can be used on virtually any system with few required libraries. The presentation includes a demonstration of the ModScan scanner as well as a rundown of the various features and modes available. I will also be covering the MODBUS and MODBUS TCP protocols including packet construction and communication flows. A brief SCADA primer is also included for the education of the audience.

Deciphering Captcha

Michael Brooks
Security Engineer, Fruition Security

This presentation will detail two methods of breaking captcha. One uses RainbowCrack to break a visual captcha. The other uses fuzzy logic to break an audio captcha. Both methods are 100% effective. These are real attacks that affect real world software: CVE-2008-2020 CVE-2008-2019. Exploit code is available to the public

CSRF Bouncing†

Michael Brooks
Security Engineer, Fruition Security

In this talk I will be discussing Exploit Chaining in Web Applications.. I will discuss the surface area problem in security and how to gain access to a greater attack surface using CSRF. As an example I will be exploiting TBDev, which is a popular private BitTorrent tracker. In this talk I will demonstrate how I found the flaws and wrote the exploit code to gain control over TBDev. I will discuss how to have fun in a sandbox and how to defend your self. I will be releasing an 0-day exploit and provide a machine for the audience to break into.

Bypassing Pre-Boot Authentication Passwords by Instrumenting the BIOS Keyboard Buffer (Practical Low Level Attacks Against x86 Pre-boot Authentication Software)

Jonanthan Brossard
Lead Security Researcher, Iviz

Pre-boot authentication software, in particular full hard disk encryption software, play a key role in preventing information theft. In this paper, we present a new class of vulnerability affecting multiple high value pre-boot authentication software, including the latest Microsoft disk encryption technology : Microsoft Vista's Bitlocker, with TPM chip enabled. Because Pre-boot authentication software programmers commonly make wrong assumptions about the inner workings of the BIOS interruptions responsible for handling keyboard input, they typically use the BIOS API without flushing or initializing the BIOS internal keyboard buffer. Therefore, any user input including plain text passwords remains in memory at a given physical location. In this article, we first present a detailed analysis of this new class of vulnerability and generic exploits for Windows and Unix platforms under x86 architectures. Unlike current academic research aiming at extracting information from the RAM, our practical methodology does not require any physical access to the computer to extract plain text passwords from the physical memory. In a second part, we will present how this information leakage combined with usage of the BIOS API without careful initialization of the BIOS keyboard buffer can lead to computer reboot without console access and full security bypass of the pre-boot authentication pin if an attacker has enough privileges to modify the bootloader. Other related work include information leakage from CPU caches, reading physical memory thanks to firewire and switching CPU modes.

Grendel-Scan: A New Web Application Scanning Tool

David Byrne
Security Consultant, Trustwave
Eric Duprey
Senior Security Engineer, Dish Network

While commercial web application scanners have been available for quite a while, the selection of open source tools has been limited. Grendel-Scan is a new tool that aims to provide in-depth application assessment. Written entirely in Java and featuring an easy to use GUI, the tool is intended to be useful to a wide variety of technical backgrounds: from IT security managers, to experienced penetration testers.

Grendel-Scan can test for authentication and authorization bypass, SQL injection (blind and error-based), XSS, CRLF injection / response splitting, session key strength, session fixation, file/directory/backup enumeration, directory indexing, web server mis-configuration, and other vulnerabilities. Exploration of the web application can be accomplished through an embedded proxy server, via automated spidering, or search engine reconnaissance.

The accuracy of the testing is increased by powerful features such as automatic detection and correction of logged out sessions, heuristic file-not-found detection, and an embedded HTML DOM parser and JavaScript engine for full page analysis. Grendel-Scan was architected with extensibility in mind. Powerful libraries offering features such as input/output tracing, session tracking, or HTML DOM comparisons make the development of new test modules much easier.

The presentation will feature an overview of the application's design, results of comparative analysis against similar tools, and a live demonstration of the tool using a real application (not an intentionally vulnerable app).

Building a Real Session Layer

D.J. Capelis

It's past time for a session layer. It's time to replace port knocking with a real authentication framework. It's time to do what DNS did with IP addresses to port numbers. It's time to run services over NATs, eliminate the need for vhosts in your webserver and provide optional transparent encryption for any client who wants it. In this talk, we'll do that and a couple other tricks... within the framework of a little-known RFC that was written almost 2 decades ago.

Hacking E.S.P.

Joe Cicero
Network Specialist Instructor, Northeast Wisconsin Technical College
Michael Vieau
Independent security researcher

Have you gone to school? Are you going to school? Do you work at a school? How do you prove you went to a particular high school, college or university? FACT: Educational institutions MUST keep your personal/confidential information. Therefore, your personal/confidential information might be at risk! This presentation will be about typical software packages found at educational institutions and their vulnerabilities. We will use known attacks to show new vulnerabilities in several typical educational software packages. The presentation will focus on the vulnerabilities, what tools were used to find them, and why successfully exploiting a weak system will allow you to gain access to a secure system.

Hacking Desire

Ian Clarke
CEO, Uprizer Labs LLC & Coordinator, The Freenet Project

What do you want? This is the question that almost every commercial organization on the planet thinks they have an answer to, but do they? Figuring out what people want is essentially a process of reverse engineering human needs, desire, and preference. It turns out that hackers are particularly adept at reverse engineering, so what happened when we applied our skills to reverse engineering what you, and everyone else, wants?

This talk will describe how we constructed a model for how the human mind decides what it wants, and then customize this model to imitate particular individuals, and thus anticipate specifically what they want. I will demonstrate the effectiveness of this approach on guessing how much particular users will like particular movies, based on the feedback they've given to a popular movie rental website. I'll also discuss flaws in how "collaborative filters" are designed, and measured, and explain why our approach is an improvement.

This talk will discuss sophisticated ideas in machine learning and artificial intelligence, but no background in these topics will be required for attendees.

Climbing Everest: An Insider's Look at one State's Voting Systems

Sandy Clark "Mouse"
University of Pennsylvania

Hanging Chads, Hopping votes, Flipped votes, Tripled votes, Missing memory cards, Machine malfunctions, Software glitches, Undervotes, Overvotes. Reports of voting machine failures flooded the news after the last elections and left most voters wondering "Does my vote really count?" "Can these electronic voting machines be trusted?" "How secure are my state's voting systems?"

In December 2007, we published an in depth, source code and hardware analysis of all the voting systems used by the state of Ohio, funded by the Ohio Secretary of State. Come find out what we learned, and draw your own conclusions.

Could Googling Take Down a President, a Prime Minister, or an Average Citizen?

Greg Conti
United States Military Academy

Every time we use the web, we disclosure tremendous amounts of information to ISPs, Internet backbone providers, and online companies; information that will be shared and data mined, but rarely discarded. Email addresses, phone numbers, aggregated search queries, cookies, IP addresses - any unique feature of our behavior provides a mechanism to link, profile, and identify users, groups, and companies. From these revelations all aspects of our daily lives emerge, including our activities, locations, and social networks. Making matters worse, ubiquitous advertising networks, dominant online companies, complicit network providers, and popular web analytic services possess the ability to track, and in some cases, eavesdrop on and modify our online communications.

The AOL dataset debacle and subsequent public outrage illustrated one facet of the problem - Search. This talk covers all aspects of the problem, including end user computers, network providers, online companies, and advertising networks. It also includes countermeasures to help protect your personal and organizational privacy. It is important to note that the research presented is the inverse of Google Hacking, which strives to retrieve sensitive information from the databases of search engines. This talk instead focuses on what information online companies can pull from you, as well as what network providers can see and modify. The long-term implications of web-based information disclosure are profound. Interaction by interaction we are ceding power to ISPs and online companies, disclosures which may one day alter the course of elections, remove world leaders from power, or cause the outspoken citizen to disappear from the web.

Compromising Windows Based Internet Kiosks

Paul Craig
Principal Security Consultant, Security-Assessment.com

Internet Kiosks have become common place in today's Internet centric society. Public Internet Kiosks can be found everywhere, from Airports, Train stations, Libraries and Hotels to corporate lobbies and street corners. Kiosks are used by thousands of users daily from all different walks of life, creed, and social status.

Internet kiosk terminals often implement custom browser software which rely on proprietary security mechanisms and access controls. Kiosks are designed to limit the level of access a user has to the Internet kiosk, and attempt to thwart malicious activity. Kiosk users are prohibited from accessing the Kiosk's local file system, or the surrounding local network attached to the Kiosk. The only guaranteed functionality is a "secured" web-browser. For a service so common-place, there has been practically zero research regarding the security of Internet Kiosk software. This talk will cover Internet Kiosk software exploitation techniques, and demonstrate multiple methods of compromising Windows based Internet Kiosk terminals.

Shifting the Focus of WiFi Security: Beyond Cracking Your Neighbor's WEP Key

Thomas d'Otreppe de Bouvette "Mister_X"
Rick Farina "Zero_Chaos"

In this talk we will discuss the paradigm shift of WiFi attacks away from the Access Points and focusing toward the clients. We will cover in depth how simple tricks such as HoneyPot Access Points or even hotspotter simply are not enough anymore and more flexible and powerful methods are being developed and used. The older, dated technologies built into Access Points for ensuring network security have failed the test of time paving way for new overlay security vendors to begin selling "Wireless Intrusion Detection and Prevention Systems" to fill the gap left by the Access Point manufacturers and the ieee802.11 committee.

We will explore a variety of feature of these devices, and see what claims stack up and which ones do not. Finally, we will explore a new frontier for WiFi networks, licensed frequencies. Many vendors currently ship ieee 802.11 compliant devices that operate on non-public bands. We will explore what types of things you can find with some simple driver modifications and why the current generation of tools needs to improve to play by these new rules. If you want to learn about what wireless hacking will look like in the coming year, instead of just cracking wep, you can't afford to miss this talk.

Hacking Data Retention: Small Sister Your Digital Privacy Self-Defense

Brenno De Winter
J.S.A.A.F., De Winter Information Solutions

Over the last couple of years a range of privacy threats have been in occurring. Europe is starting to look like the playing field of what

is to come to the US: Storage of all e-mail traffic, online presence, phone calls, actual traveling throughout nations and filtering of content. Fortunately a closer look at the measures shows that it is never smart to overestimate the abilities European governments have and digital self defense is possible. But since we don't want to underestimate the threat as well. So that's why we look how these measures effects can be greatly reduced and how we can have fun online again. This knowledge is something we probably want to extend to many people to help them reclaim their digital rights with the use of simple and existing technologies. The Small Sister Project shows you how to do that and delivers the tools to make that easier. Learn how simple measures can make a huge difference.

Security and Anonymity Vulnerabilities in Tor: Past, Present, and Future

Roger Dingledine

Project leader, The Tor Project

There have been a number of exciting bugs and design flaws in Tor over the years, with effects ranging from complete anonymity compromise to remote code execution. Some of them are our fault, and some are the fault of components (libraries, browsers, operating systems) that we trusted. Further, the academic research community has been coming up with increasingly esoteric — and increasingly effective! — attacks against all anonymity designs, including Tor.

Roger will walk through some of the most egregious bugs and design flaws we've had, and give some intuition about lessons learned building and deploying the largest distributed anonymity network ever. Then he'll outline the wide variety of current vulnerabilities we have, explain what they mean for our users, and talk about which ones we have a plan for and which ones will continue to be a pain for the coming years. Last, we'll speculate about categories and topics that are likely to introduce new problems in the future.

Next Generation Collaborative Reversing with Ida Pro and CollabREate

Chris Eagle

Associate Chairman of the Computer Science Dept, Naval Postgraduate School (NPS)

Tim Vidas

Research Associate, Naval Postgraduate School (NPS)

A major drawback with the use of most reverse engineering tools is that they were not designed with collaboration in mind. Numerous kludgy solutions exist from asynchronous use of the same data files to working on multiple copies of data files which quickly diverge leaving the differences to somehow be reconciled. Pedram Amini's Ida Sync provided a first step towards automated collaboration among Ida users however Ida Sync suffers from several shortcomings including the fact that it has failed to keep pace with the evolution of Ida's internal architecture. In this presentation, the authors present a new tool titled collabREate designed to bring nearly effortless collaboration to Ida users. The talk will include discussion of the IDA API and the ways in which it facilitates collaboration along with the ways in which it hinders collaboration. The design of a robust server component, responsible for managing projects and connected clients will also be discussed along with a number of capabilities beyond simple collaboration that are enabled via the collabREate architecture.

Markets for Malware: A Structural Economic Approach

Brian K. Edwards

Economist, Los Alamos National Laboratory

Silvio J. Flaim

Economist, Los Alamos National Laboratory

Much literature has addressed the issue of the relative sizes of shadow economies in different countries. What is largely missing from this discussion is a more structured discussion on how to incorporate estimates of shadow economic activity into the national income accounting framework and a discussion of how the shadow components of specific industries can be analyzed in either an input-output or macroeconomic framework. After a brief discussion of existing estimates of black market activity, we discuss how black market activities might be measured and incorporated in standard economic models of the economy. We then focus particular attention on the malware industry and discuss how malware activity influences other economic activity (both official and shadow) and discuss possible methods of how malware activity can be estimated, and how the contribution of malware to overall economic activity can be measured. Finally, we discuss how the methods used to integrate malware economic activity into the national income accounts can be applied to other sectors of the economy, and hence how to develop an alternative measure of the size of the shadow economy. With a new baseline incorporating these "shadow" activities, the economic model is used to examine questions such as: What is the net economic contribution of malware and other shadow economic activity? What would be economic impact of eliminating malware and other shadow activity in all its forms?

De-Tor-iorate Anonymity

Nathan Evans

Ph.D Student, University of Denver

Christian Grothoff

Feel safe and comfortable browsing the Internet with impunity because you are using Tor? Feel safe no more! We present an attack on the Tor network that means that the bad guys could find out where you are going on the Internet while using Tor. This presentation goes over the design decisions that have made this attack possible, as well as show results from a Tor network that reveals the paths that data travels when using Tor. This method can make using the Tor network no more secure than using a simple open web proxy. We go over the attack in detail, as well as possible solutions for future versions of Tor.

Identification Card Security: Past, Present, Future

Doug Farre

Administrative Director, Locksport International

Come learn how identification cards have taken over our lives, how they can be manufactured at home, and how you can start a legal ID making business. Come learn all the tips and tricks about amateur id manufacturing and pickup the first ever Complete Amateur ID Making Guide. Also, come test your ability to spot a fake, vs. a real, and check out the newest in ID technology. Polycarbonate laminates, biometrics, Teslin, and RFID. Lastly, see how corporations are affecting the identification card fiasco in the U.S. What's in your wallet?

Snort Plug-in Development: Teaching an Old Pig New Tricks

Ben Feinstein

Security Researcher, SecureWorks Counter Threat Unit

Snort has become a standard component of many IT security environments. Snort is mature and widely deployed, and is no longer viewed as new or exciting by the industry. However, with such widespread deployment, enhancing Snort's capabilities offers the potential for a large and immediate impact. Instead of chasing the industry's new-hotness of the day, it frequently makes more sense to add new capabilities to an existing security control.

With this in mind, the author set out to implement new and innovative capabilities in the form of GPL-licensed Snort plug-ins. The author will introduce the Snort plug-in architecture and the relevant APIs used when implementing extensions to Snort. Lessons learned and pitfalls to avoid when developing Snort plug-ins will be covered. Some interesting code snippets will be discussed. Ideas for future work in the area of Snort extensions will be presented.

The Wide World of WAFs

Ben Feinstein

Security Researcher, SecureWorks Counter Threat Unit

With webapp protection now mandated by the PCI standard, web-application firewalls (WAFs) have received newfound interest from both consumers of security technologies, as well as from security researchers and potential attackers. Now that WAFs are a PCI-approved substitute for code reviews, expect many vendors to opt for this potentially less costly route to compliance. Of course, security researchers and potential attacks will increasingly train their sights on this lucrative and expanding target.

This talk will explore the ModSecurity Apache module and how it is being used as a WAF to meet the PCI 6.6 webapp protection requirement. The relative strengths and weaknesses of WAFs in general and ModSecurity in particular will be highlighted. Common deployment scenarios will be discussed, including both in-the-cloud, stand-alone and Apache server embedded deployments. The ModSecurity rules language will be covered and several ModSecurity Core Rules that are representative of its capabilities will be dissected in depth. Finally, some interesting uses of ModSecurity's content injection capabilities will be discussed. Anyone up for hacking the hacker via scripting injected into your webapp's response to an attempted attack? This talk will show you how!

VLANs Layer 2 Attacks: Their Relevance and their Kryptonite

Kevin Figueroa

CEO & Information Security Engineer, K&T International Consulting, Inc.

Marco Figueroa

CEO & Senior Security Analyst, MAF Consulting, Inc.

Anthony L. Williams

CEO & Information Security Architect, IRON::Guard Security, LLC

Proper network infrastructure configuration is a crucial step in a successful defense in depth strategy for any organization. The fact that the network fabric is susceptible to these attacks years after their initial discovery is alarming and disgusting at the same time. We propose to revisit these attacks using contemporary techniques and tools and also offer equally contemporary solutions to mitigate or foil these malicious networks attacks as the case may be. Networking professionals will be able to walk away from this presentation with solid remedies to these issues with a reinforcement that they actually still exist and are pertinent to a network security strategy that will function now and in the future.

Virtually Hacking

John Fitzpatrick

Information Security Consultant - MWR InfoSecurity

Own the VMware box and you get half the servers on the network for free. Although, depending on the VMware server's configuration, whether you want to be stealthy about it and whether you want to avoid any disruption it may not always be quite that simple. During this talk we will take a look at ways of jumping from a server to guest OS without causing any disruption and also some tools for assessing the security posture of VMware products.

With VMware becoming an integral part of many networks it is important that the security level of its deployment is assessed appropriately. Without the right tools to do the job this can be a slow and painful task; with the right tools you can have a lot of fun. I'll demo some tools which I have been working on that harness the power of dradis and make testing and possibly owning VMware servers and VMs a virtually painless task.

Is That a Unique Credential in Your Pocket or Are You Just Pleased to See Me?

Zac Franken

Security Researcher

This year new shiny toys are abound, as I'll tell you about the credentials in your wallet, and even in you. How secure (or not) they are and a few ways to duplicate / replicate /emulate them.

Last year at Defcon 15 I had a bit of a chat with you guys and gave you an overview of access control systems, told you of their common flaw, and showed you some cool toys that exploit it. This year, from the humble magnetic stripe card to the modern hand geometry scanner, I will take you through some simple (and not so simple) ways to get in, so you can try and keep them out.

Physical access control systems are shockingly vulnerable. As far as I am concerned most have the security equivalence of a "Please keep off the grass" sign.

Take that "Please keep off the grass" sign, add poor implementation, bad products, and a security industry that charges extra for any security whatsoever, poor locks that are pickable/bumpable, add accountants that nickel and dime their organization's security budget (because it doesn't have to be secure, it just has to enable them to tick a box in their corporate filings), and you end up with a sign that says "eep ass" which only delays an intruder in as much, as they briefly stop to ponder WTF you meant by the sign in the first place. Why are you here? Why aren't you at home on the porch with a shotgun protecting your property?!

Wait a minute..... Why am I here?!

Exploiting A Hundred-Million Hosts Before Brunch

Stefan Frei

Security Researcher

Thomas Duebendorfer

Security Researcher

Gunter Ollmann

Security Researcher

Martin May

Security Researcher

If you were to "hack the planet" how many hosts do you think you could compromise through a single vulnerable application technology? A million? A hundred-million? A billion? What kind of application is so ubiquitous that it would enable someone to launch a planet-wide attack? - why, the Web browser of course! We've all seen and studied one side of the problem - the mass- defacements and iframe injections. But how many vulnerable Web browsers are really out there? How fast are they being patched? Who's winning the patching race? Who's the tortoise and who's the hare? Our latest global study of Web browser use (tapping in to Google's massive data repositories) has revealed some startling answers along with a new perspective on just how easy it would be to "hack the planet" if you really felt like it.

Paper Download and Contact

W: http://www.techzoom.net/insecurity-iceberg
M: insecurity-iceberg@ee.ethz.ch

Nmap: Scanning the Internet

Fyodor

Hacker, Insecure.Org

Nmap was built to efficiently scan large networks, but we have lately taken this to a new level with massive scans of the IPv4 Internet. We hope to finish scanning a significant portion of the Internet (if not the whole thing) in time for Defcon as part of our Worldscan project. Nmap author Fyodor will present our most interesting findings and empirical statistics from these scans, along with practical advice for improving your own scan performance. Additional topics include detecting and subverting firewall and intrusion detection systems, dealing with quirky network configurations, and advanced host discovery and port scanning techniques. A quick overview of new Nmap features will also be provided.

Journey to the Center of the HP28

Travis Goodspeed

Security Researcher

In 1990, a wire-bound book was published in Paris by the title of <<Voyage au centre de la HP28 c/s>>. It presents a very thorough account of the inner workings of the Hewlett Packard 28 series of graphing calculators. Designed before the days of prepackaged microprocessors, the series uses the Saturn architecture, which HP designed in-house. This architecture is very different from today's homogeneous RISC chips, with registers of 1, 4, 12, 16, 20, and 64 bits in width. The fundamental unit of addressing is the nibble, rather than the byte. Floats are represented as binary-coded decimal, and a fundamental object in the operating system is an algebraic expression.

This architecture is still used, albeit in emulation, in the modern HP50g. With this talk, I intend to call attention to a fascinating, professional, and well-documented feat of reverse engineering. Using little more than their ingenuity and an Apple][e, Paul Courbis and Sebastien Lalande reverse engineered a black box calculator into a real computer, one which became user-programmable in machine language as a result. More than that, they documented the hack in such exquisite detail that their book is not just a fascinating read, but also veritable holy scripture for anyone trying to write custom software for this machine.

Expect a thorough review, in English, of the contents of the book. This is not a sales pitch; electronic copies of both the translation and the original are free to all interested readers. Topics include the datatypes of the computer algebra system, hacking an upgrade into the memory bus, bootstrapping an assembler, writing in machine language by tables, and adding an I/O port for software backups.

Making the DEFCON 16 Badge

Joe "Kingpin" Grand

For the third year in a row, Kingpin has had the honor of designing the DEFCON Badge. No longer just a boring piece of passive material, the badge is now a full-featured, active electronic product. If you're up early enough and interested in details of the entire development process of the badge, from initial concept drawings to prototype electronics to completed units, and want to hear stories of the trials and tribulations that come with designing and manufacturing, be sure to come to this talk.

BSODomizer

Joe "Kingpin" Grand

Zoz

Robotics Engineer

We like hardware and we like messing with people. BSODomizer lets us do both. BSODomizer is a small propeller-based electronic device that interfaces between a VGA output device (laptop or desktop) and VGA monitor and will flash images at random time intervals. (Surprise Goatse!) Or display your favorite BSOD causing the confused user to turn off their machine over and over again. Customization for different modes are configurable via on-board DIP switches.

We'll bring you through the entire design and development process of the device and end with some never-before-seen footage of poor bastards taking the bait. Full schematics, firmware, circuit board layout, and bill of materials will be released, so you can build your own BSODomizer. We'll have some bare PCB's and parts available for your instant gratification.

Don't let the name fool you. BSODomizer will do everything you've always wanted to do to your enemies (or friends) without the messy cleanup.

Nail the Coffin Shut, NTLM is Dead

Kurt Grutzmacher

Security Researcher

Ever since SirDystic's SMBRelay release the weaknesses of the NTLM protocol have been repeatedly shown. For over twenty years this protocol has been refined by Microsoft, it's time to let it go and stop supporting it within our networks.

This presentation will trace the history of the NTLM protocol and the various attacks that have befallen it over the past decade, the attempts at fixing them and why these fixes have not succeeded. I will show what I believe is the most significant attack to it and why the best solution is to migrate away from NTLM once and for all. Attendees will come away with a stronger understanding of the NTLM protocol and information to help them make the case to their Windows administrators, CIOs, CSOs and everybody else that there is a serious risk in keeping NTLM support around. A toolkit using the Metasploit Framework will be released that will help you show the risks in your enterprise.

Satan is on my Friends list: Attacking Social Networks

Nathan Hamiel

Senior Consultant, Idea Information Security

Shawn Moyer

CTO, Agura Digital Security

Social Networking is shaping up to be the perfect storm... An implicit trust of those in one's network or social circle, a willingness to share information, little or no validation of identity, the ability to run arbitrary code (in the case of user-created apps) with minimal review, and a tag soup of client-side user-generated HTML (Hello? MySpace? 1998 called. It wants its markup vulns back). Yikes.

But enough about pwning the kid from homeroom who copied your calc homework. With the rise of business social networking sites, there are now thousands of public profiles with real names and titles of people working for major banks, the defense and aerospace industry, federal agencies, the US Senate... A target-rich and trusting environment for custom-tailored, laser-focused attacks.

Our talk will show the results of a series of public experiments aimed at pointing out the security and privacy ramifications of everyone's increasingly open, increasingly connected online personae and the interesting new attack vectors they've created.

Plus, we get to have some fun violating scads of EULAs, AUPs, and Terms of Service along the way.

K. THX FOR THE ADD!!1!

YOU RAWK.

Advanced Software Armoring and Polymorphic Kung Fu

Nick Harbour

Principal Consultant, Mandiant

This presentation discusses the techniques employed by a new anti-reverse engineering tool named PE-Scrambler. Unlike a traditional executable packer which simply compresses or encrypts the original executable, this tool has the ability to permanently modify the compiled code itself. With the ability to modify compiled programs at the instruction level a vast array of Anti-Reverse Engineering techniques are possible that would traditionally have been performed only by hand by seasoned hackers. In addition to thwarting a would-be reverse engineer, the tool has the ability to randomly modify code in a program in a fashion that keeps the functionality of the program intact. This is useful for modifying a program to defeat signature recognition algorithms such as those used in Anti-Virus programs. In this presentation we will discuss several of these Anti-Reverse

presentations cont.

Engineering and Polymorphic techniques in depth. A new technique and tool for detecting armored and packed binaries will also be discussed and demonstrated.

In addition to learning about two new security tools, attendees will learn state-of-the-art anti-disassembly and anti debugging techniques. Attendees' eyes will be opened to the vast world of possibility that lies in the future for binary armoring and develop a true contempt for the binary packers of today.

A Hacker Looks at 50

G. Mark Hardy
Founder, National Security Corporation

Take a trip back in time and discover what hacking was like in the pioneer days — before the Internet, the PC, or even the Commodore 64 or TRS-80. The speaker started "exploring" computer systems in 1973, when the only law about hacking was the hacker ethic itself. Join a humorous reminiscence about what it was like building an Altair 8800, "discovering" the 2600 Hz tone, storing programs on punched cards, cracking bad crypto, and more. You'll find the people and principles haven't changed, only the speed of the hardware.

Playing with Web Application Firewalls

Wendel Guglielmetti Henrique
Penetration Test Analyst - Intruders Tiger Team Security

WAF (Web Application Firewalls) are often called 'Deep Packet Inspection Firewalls' because they look at every request and response within the HTTP/HTTPS/SOAP/XML-RPC/Web Service layers. Some WAFs look for certain 'attack signatures' to try to identify a specific attack that an intruder may be sending, while others look for abnormal behavior that doesn't fit the websites normal traffic patterns. Web Application Firewalls can be either software, or hardware appliance based and are installed in front of a webserver in an effort to try and shield it from incoming attacks.

Today WAF systems are considered the next generation product to protect websites against web hacking attacks, this presentation will show some techniques to detect, fingerprint and evade them. Affiliated to Hackaholic team (http://hackaholic.org/) and working as penetration tester to a Brazilian company called SecurityLabs in the Intruders Tiger Team division - One of leaders company of segment in Brazil, among our clients are government, credit card industry, etc.

War Ballooning — Kismet Wireless "Eye in the Sky"

Rick Hill
Senior Scientist, Tenacity Solutions, Inc.

Using a Balloon as an aerial network surveillance platform, a.k.a. "WarBallooning" is an idea that evolved as a natural progression out of my Rocket-based experiment @ Defcon 14 entitled, "WarRocketing - Network Stumbling 50 sq. miles in < 60 seconds."

Interestingly, after my presentation in 2006, many in the wireless community discussed Balloon-based network discovery, notably CoWF & Slashdot. But, alas, like many great concepts in the scientific community, I found after much research (2008) that sadly to my (& Google's) knowledge no one has yet demonstrated WarBallooning ... Until Today!

My team, (with the help of CoWF and DEFCON support staff) will demonstrate WarBallooning @Defcon 16 over the Riviera Hotel. Wardriving coverage is limited by obstructions such as trees, houses, and terrain. Our latest aerial platform, (a 6 ft. Helium Balloon) does not have these limitations. Essentially, it was built to provide a superior Line-of-Sight, enabling the Wardriver to rapidly recon. a fairly large urban area.
Most Notable Feature: The Kismet "Eye in the Sky" actually beams live video back as the antenna targets various buildings (& networks.) The presentation will include details of all hardware hacks involved in the construction: WRT54G, Alchemy, Kismet Drone, & IP camera modifications. No prerequisite - only an interest in Network Stumbling and Wireless Technology.

Under the iHood

Cameron Hotchkies
Vulnerability Analysis, TippingPoint

The market share for Apple devices has grown considerably over the past few years, but most reverse engineering topics still focus on Microsoft platforms. This talk will outline what is necessary to begin reversing software on OS X. This will include a rundown of the tools available to an apple based researcher, how Objective-C works and what it looks like in a binary, the basics of the Mach-O file format including the undocumented _OBJC section and comparisons of Windows applications and the OS X counterparts.

Race-2-Zero Unpacked

Simon Howard
Founder, Mince Research

Signaure-based Antivirus is dead, we want to show you just how dead it is. This presentation will detail our findings from running the Race-2-Zero contest during DC16. The contest involves teams or individuals being given a sample set of malicious programs to modify and upload through the contest portal. The portal passes the modified samples through a number of antivirus engines and determines if the sample is a known threat. The first to pass their sample past all antivirus engines undetected wins that round. Each round increases in complexity as the contest progresses.

Topics covered will include:

- An overview of the multi-AV engine interface
- Mutation / obfuscation techniques
- Statistical analysis of the time taken to circumvent various products
- Different approaches used by contestants
- Were viruses or exploits easier to obfuscate?

Prize giving ceremony with celeb judging panel... prizes will be awarded for:

- The most elegant solution
- Comedy value
- Dirtiest hack
- ... and most deserving of a beer

The Death of Cash: The loss of anonymity and other dangers of the cash free society

Tony Howlett
President, Network Security Services

In this talk, we will discuss the pros and cons (mostly cons) of the cash less society and how it might endanger your privacy and civil liberties. This movement towards the elimination of cash has been picking up speed and mostly accepted by the populace as a huge convenience. We examine some reasons why this isn't such a good thing. We also look at legislation and laws in this area that give banks and the government unprecedented ability to track your financial transactions, cash and non with little or no cause. And finally some ways to avoid this scrutiny and protect your financial privacy.

Ham For Hackers — Take Back the Airwaves

JonM
Security Consultant & Amateur Radio Operator

Think amateur radio is all about dorks with walkie talkies? Think again. Amateur radio presents one of the last bastions for open radio experimentation. This talk will provide a brief introduction to amateur radio, explain the advantages of licensed spectrum for experimentation, and describe how to get involved in the leading edge of radio hacking.

Demonstration of Hardware Trojans

Fouad Kiamilev
Professor, Electrical & Computer Engineering Dept., University of Delaware
Ryan Hoover
Graduate Student

Recent developments such as the FBI operation "Cisco Raider" that resulted in the discovery of 3,500 counterfeit Cisco network components show the growing concern of U.S. government about an electronic hardware equivalent of a "Trojan horse". In an electronic Trojan attack, extra circuitry is illicitly added to hardware during its manufacture. When triggered, the hardware Trojan performs an illicit action such as leaking secret information, allowing attackers clandestine access or control, or disabling or reducing functionality of the device. The growing use of programmable hardware devices (such as FPGAs) coupled with the increasing push to manufacture most electronic devices overseas means that our hardware is increasingly vulnerable to a Trojan attack from potential enemies.

This talk explores three possible methods that a hardware Trojan can use to leak secret information to the outside world: thermal, optical and radio. The hardware platform for our demonstration is a $149 Spartan-3E Starter Kit from XILINX. The application used in our demonstration is AES encryption. The objective of our Trojan is to illicitly leak the AES encryption keys once triggered.
In the thermal Trojan demo, we use an infrared camera to show how electronic components or exposed connector pins can be used to transmit illicit information thermally. In the optical Trojan demo, we use an optical-to-audio converter to show how a power-on LED can be used to transmit illicit information using signal frequencies undetectable by human eyes. Finally, in the radio Trojan demo, we use a radio receiver to show how an external connector can be used to transmit illicit information using AM radio transmission.

We finish our talk with a demonstration of an optical Trojan that leaks the encryption keys from a popular commercial network router (e.g. Cisco-Linksys WRT54GS).

WhiteSpace: A Different Approach to JavaScript Obfuscation

Kolisar
Security Researcher

A different approach to JavaScript obfuscation will be presented. There are certain telltale indicators within an obfuscated JavaScript file which can be used for detection and protection. These signs occur in almost all obfuscated JavaScript and are easily detected via software and visual inspection. This different approach addresses these telltale indicators and provides a method of JavaScript obfuscation which hides these indicators from both automated and visual inspection.

Flux on: EAS (Emergency Alert System)

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

Discover the great mystery that is the Emergency Alert System. An elaborate way for the President of the United States to have his or her voice heard from every broadcast outlet at the same time. It can also perform other less important rolls such as letting the public know when their lives may be in danger by several natural occurring and man made events.

DNS Goodness

Dan Kaminsky

Career Mythbusters: Separating Fact from Fiction in your Information Security Career

Lee Kushner
President, LJ Kushner and Associates, LLC
Mike Murray
Director of Neohapsis Labs

How long should my resume be? Do I really need to be a Manager? Do I need to attend business school? What certifications do I need? Does my title matter? Should I go after money or a cool job? What are the hot skills du jour? How do I use LinkedIn and Facebook? All of these questions are asked continually by Information Security professionals as they assess their current positions and determine which future opportunities align with their aspirations. Mike Murray and Lee Kushner return to the DefCon stage to answer these questions and dispel the prevailing myths that permeate the information security industry. Participants should leave the presentation with a better way to map out their own career and separate fact from fiction as they make decisions on how to pursue their ultimate career goals.

Taking Back your Cellphone

Alexander Lash
Security Researcher

This presentation will cover a variety of topics of interest to anyone on a cellphone network in the US. I'm going to cover how to use your own backends for MMS and WAP access, unlock Bluetooth tethering, and circumvent some of the more obnoxious carrier restrictions.

Of course, the best part is baking your own firmware and running your own code. I'll provide an overview of the processes necessary to do so, a quick rundown of what you can expect from your carrier, a few tools and docs I've assembled to take a little pain out of the process, and all of the information you'll need to void your warranty with gusto and panache.

I'll provide several demonstrations you can follow along with on your own phone. The more restricted your phone is, the more mileage you'll get out of this talk — and one lucky audience member will have their warranty voided live!

Comparison of File Infection on Windows & Linux

lclee_vx
Founder F-13 Labs
lychan25

This talk documents the common file infection strategies that virus writers have used over the years, conduct the comparison of Portable Executable (PE) file infection on the Windows platform and Executable and Linking Format (ELF) file infection on the Linux Platform.

Developments in Cisco IOS Forensics

"FX" Felix Lindner
Head of Recurity Labs

Attacks on network infrastructure are not a new field. However, the increasing default protections in common operating systems, platforms and development environments increase interest in the less protected infrastructure sector. Today, performing in-depth crash analysis or digital forensics is almost impossible on the most widely used routing platform.

This talk will show new developments in this sector and how a slightly adjusted network infrastructure configuration together with new tools finally allows to separate crashed, attacked and backdoored routers from each other. We walk through the known types of backdoors and shellcodes for IOS as well as their detection and the challenges in doing so.

Malware RCE: Debuggers and Decryptor Development

Michael Ligh
Security Intelligence Engineer, iDEFENSE
Greg Sinclair
Rapid Response Engineer, VeriSign iDefense Rapid Response

This talk will focus on using a debugger to reverse engineer malware, with an emphasis on building decryption tools for credential recovery and command/control (c&c) inspection. Most modern-day trojans exhibit cryptography, or just home-grown obfuscation techniques, to prevent analysis of the stolen data or c&c protocol. This presentation will show how to script the debugger such that it leverages the trojan's own internal functions to decrypt information of the researcher's choice. The concepts will be demonstrated using current threats such as Feebs, Silent Banker, CoreFlood, Torpig/MBR, Kraken, Prg/Zues, and Laqma.

Tuning Your Brain

Lyn

I can't tell you how often I'm listening to trance, goa or industrial when I'm coding. Often when we're stuck in a black hole, or just can't figure the problem out - the right music will help. Why does this work? It seems motivating, and it seems like we solve problems easier, and it seems to create a flow. Turns out, your brain is like a tuning fork. This talk will include a bit of biology - going over the basics of the brain structures, neurons, synapses and neurotransmitters, before getting to how music affects the brain, and how it helps us think.

Feed my Sat Monkey

Major Malfunction

In this confused rant^W^W talk, I will explain why the little green men are right, and also know how to party. I will show you some new toys. Shiny ones. Ones that go 'beep' and have flashy lights. You will like it, and I will be able to return to my home planet, mission accomplished, to the adulation of the triple-breasted masses and the reward of a grateful nation, followed by tea, medals and an inadequate state pension. Or I'll go to jail, whichever's quicker and/or cheaper.
OK, so you've sated your almost bottomless appetite for pr0n, obscure sports, late night poker and reality TV from countries you've never heard of and hopefully will never have to visit, so what else is there to do? What else is up there? (Apart from little green men, obviously... which are completely real, BTW... You should see some of the stuff we've got over in... oh, wait... I'm not supposed to talk about that...) Where was I? Oh, yes... so I've got about a gazillion channels on a trillion satellites all bobbing about above me in space, but what are they all doing? How can I find anything interesting amongst all that background noise? Enough with the pr0n already! I want to see something cool! I want something nobody else is getting! I want what THE MAN's got!!! I want to be able to say to my friends "It just comes to you... This stuff just flies through the air... They send this information out - it's just beamed out all over the fuckin' place... All you have to do is know how to grab it... See, I know how to grab it.". And stuff like that. Yeah, baby. That would be HOT!

I'll also talk about something else. Something that'll probably get me whacked. So let's not talk about it yet, eh?

Fear, Uncertainty and the Digital Armageddon

Morgan Marquis-Boire
Principal Consultant, Security-Assessment.com

We now live in an age where attacks on critical infrastructure will cause real world harm. An increasing global concern regarding cyber-terrorism reflects the problem critical infrastructure security poses for many large IT consulting companies, telecommunications providers, utilities and industrial companies.

SCADA networks are the foundation of the infrastructure which makes everyday life possible in most first world countries. This talk will provide an introduction to critical infrastructure environments and SCADA networks and the major differences that exist between understood security best practice and the protective measures regularly found (or not) in these networks.

The most common security mistakes will be covered, as will real world examples taken from penetration testing SCADA environments. Additionally, this talk will expose some of the potentially catastrophic consequences of a failure in a production SCADA environment. There will be an examination of the critical infrastructure hysteria which is currently in vogue and some consideration of steps which can be taken to secure these networks and prevent cyber-terrorism.

Sniffing Cable Modems

Guy Martin
Security Researcher

Cable modems are widely used these days for internet connections or other applications. This talk gives a detailed overview of this mean of communication with a focus on its security.

DOCSIS (Data Over Cable Service Interface Specification) is currently the most used protocol around the world for providing internet over TV coaxial cable. Due to its nature, this protocol can easily be sniffed by taping onto the TV cable using a digital TV card. By doing this, you can not only sniff your own connection but all the connections of the entire neighborhood. With my tool packet-o-matic and an inexpensive DVB-C card, countless things are possible ranging from dumping people's email into maildir to removing firewall rules and quota limitation on your connection or even a DoS of all HTTP communications by injecting TCP reset packets.

Toasterkit, a Modular NetBSD Rootkit

Anthony Martinez
Systems Administrator, New Mexico Tech
Thomas Bowen
Systems Administrator, New Mexico Tech

NetBSD is a portable operating system for just about every architecture available. There is a notable lack of tools available for the penetration tester. In this talk we will present Toasterkit, a generic NetBSD rootkit. It has been tested on i386, Mac PPC, and VAX systems.

Bringing Sexy Back: Breaking in with Style

David Maynor
CTO, Errata Security
Robert Graham
CTO, Errata Security

Security is getting better; there is no doubt about that. High value targets are increasing their security while buying into the buzzword hype with phrases like "defense in depth". Firewalls, IPS, AV, NAC, and a host of other technologies have done a lot to give the pointy hair bosses of the world the ability to sleep easy...or has it. While those PHB sleep easy in their bed the ability to compromise a site at will continues to grow.

Remember the good old days of planting Trojans in microcontrollers of your enemy's hardware or shipping packages with system updates that contain backdoors? What happened to those days? What if I told you that breaking into a site is as easy as sending a package via some third party carrier or throwing up a website. This talk will cover penetration techniques that at first glance appear to be Hollywood fiction but are easy and reliable methods of intrusion.
Miss this talk and you may never know why you have a package in your shipping department addressed to "U R Owned, INC.".

Forensics is ONLY for Private Investigators

Scott Moulton
President of Forensic Strategy Services, LLC

If the only requirement for you to become a Computer Forensic person is to be a Private Investigator, why would you ever take a certification again? You would never need to be a CCE (computer certified examiner), nor any other certification of any kind. You would be one of the only people in your area that could legally do the job and why spend a single dime you don't have to? These new laws will destroy certifications and qualifications as we know it, and we will be pushed out of our own industry!

I was the one of the first experts to be challenged on the new Private Investigator laws while on the stand testify in a criminal case in 2006. This is the bill that actually passed in 2006 a week before I took the stand and was challenged by state prosecution. It simply states that doing any kind of 'digital investigation' without a PI license is a felony.
http://www.legis.state.ga.us/legis/2005_06/fulltext/hb1259.htm

When they passed the law in March of 2006 they intended for it to go into effect on July 1st, 2006 with no grandfather clause. Since it takes 2 years to become a PI in the state of Georgia, immediately everyone that was a third party practicing forensics would be a felony.

In Georgia it is a 2 year apprenticeship, then a test and a pile of money and insurance (PI's have to have 2 million in EandO) and then 40 hours of continuing education a year specifically on PI topics in certified classes. Currently I do not know of any on computer forensics that qualify for the PI continuing education. The inclusion of computer forensics in the PI license does not change a single item for the existing PI tests, knowledge base, or requirements. A security guard would be able to do a computer forensic job legally where the CISSP could not.

Since this time, my company has become a Private Investigation company and I have a Private Investigator License. This is a talk about the struggles of becoming a PI and what the laws are for computer forensics going forward. Everyone that does computer security for any legal purpose, or computer forensics as a third party stands to lose as these laws are being passed all over the United States. In the future it may be impossible for "you" to go out on your own doing any kind of "DIGITAL" security or forensic work limiting your future forever!

I hope that everyone who never pays any attention to legislation and their own laws, spends a little time reviewing the laws they are trying to slip in without your even knowing it is coming. There is a great ignorance amongst computer security and computer forensic people that just disbelieves this can even happen. However a few states like Texas have already made this a law and it is affecting the industry now and causing quite a few well know computer forensic people to walk away from jobs. I hope everyone listens and gets involved and joins together this fragmented society of computer security and forensic people into one voice that makes the states take notice that we will not standby and let government make our choices for our future!
If you are in a computer forensic job or collect any kind of digital evidence for any legal purpose you might want to be aware of what is about to happen to your jobs! Now is the time to get knowledgeable about this topic and do what you can to prevent it from becoming the requirement for you to have a job. Computers Forensics/Security and Private Investigations are so different that many people will never believe that is what will enable you to be able to do your job. This will destroy certifications as we know it for many digital fields.

Solid State Drives Destroy Forensic & Data Recovery Jobs: Animated!

Scott Moulton
President of Forensic Strategy Services, LLC

This speech is all ANIMATION in 3D! Data on a Solid State Device is virtualized and the Physical Sector that you are asking for is not actually the sector it was 5 minutes ago. The data moves around using wear leveling schemes controlled by the drive using propriety methods. When you ask for Sector 125, its physical address block is converted to an LBA block and every 5 write cycles the data is moved to a new and empty previously erased block. This destroys metadata used in forensics & data recovery. File Slack Space disappears, you can no longer be sure that the exact physical sector you are recovering was in the same location or has not been moved or find out what it used to be!
I will explain how Flash and Solid State Drives are different and compare them to hard drives in their ability to read and write data. What happens when they are damaged and a recovery needs to be done? In this process you will see how the data gets shuffled around and how some of the data is destroyed in the process making it impossible in many cases to recover some files and metadata that on a hard drive has been a simple task by comparison. You will also get an idea about how propriety methods that each vendor is using will isolate you from knowing what is happening to your data or even where it is on the drive. And at the very least the animation is the quality of the History Channel and you will enjoy what you are learning!

Beholder: New Wifi Monitor Tool

Nelson Murilo
Security Researcher
Luiz 'effffn' Eduardo
Security Researcher

Although it's not something new at all, network administrators are still facing (and having to deal) with old problems and threats. One of these problems is to be able to detect rogue and/or fake access points in their networks and surroundings. The current solutions available are mostly commercial and/or proprietary, but we haven't seen yet any open-source tool that implements specifically WIDS capabilities. We would like to introduce to DefCon: Beholder. The talk will include a brief introduction on the general state of the commercial WIDS tools and evolution of wireless attacks, and will be mostly focused on the Beholder project. Beholder is an C language opensource tool available (for now) for linux platforms, and it can be used for any available 802.11 technology a nic card may support, and it isn't driver dependent, run in all available linux wifi drivers. The tool does some, of course, some basic network scanning, but also implements some simple (but cool) stuff, that some of the commercial tools don't have. The presentation will cover details about that tool, future features, scenarios to be implemented, examples, and a demo (yep, demo at DefCon) of malicious AP/tools in action and how beholder can be used to detect it.

Good Viruses. Evaluating the Risks

Dr. Igor Muttik
Sr. Architect McAfee Avert Labs

This session will discuss the risks associated with creation of replicating code. A combination of wide availability of virus source code as well as the problem of control over replicating code make these experiments quite risky. To demonstrate these points we shall see how a computer virus was once created unintentionally in a self-modifying tool called ALREADY.COM (we'll disassemble and debug it). We shall watch a video of the "Corrupted blood" epidemic in World of Warcraft when a virtual "good" virus got out of control. We will examine "beneficial" properties of W32/Nachi worm and discuss pros and cons of harnessing replication for patching vulnerabilities.

Brain Games: Make your own Biofeedback Video Game

NeOnRa1n
Joe "Kingpin" Grand
Founder, Grand Idea Studios

More and more scientific studies are weighing in on video games and their positive benefits. The dated idea of video games being damaging to one's health and a waste of time is slowly being replaced with the idea of video games as high-tech therapy. By incorporating sensors to measure the player's physiological state, game play performance can be affected or altered. Among the various types of biofeedback, heart rate variability is one of the easiest to understand and build hardware for. In this presentation, not only will we guide you through how to construct simple hardware to read your own heart rate and provide you with some open-source code as a starting point for your future favorite biofeedback game designs, we will also use a real-live human volunteer from the audience to demonstrate the technology!

Anti-RE Techniques in DRM Code

Jan Newger
Security Researcher

In order to prevent music from being copied among consumers, content providers often use DRM systems to protect their music files. This talk describes the approach taken while analysing a DRM system (whose identity needs to be kept secret due to legal issues). It is shown what techniques were used to protect the system from being easily reverse engineered. This is not about how to hack $Insert_DRM_Here. No decryption tools or information on how to write one will be released.

VoIPER: Smashing the VoIP Stack While you Sleep

N.N.P.
Hacker, UnprotectedHex.com

With VoIP devices finding their way into the majority of major enterprises and a significant number of residential installations, the possible consequences of a security vulnerability that can be leveraged by malicious hackers are ever increasing. While the security of data and voice traffic has been extensively promoted and tested the security of the devices themselves has been poorly tested at best. A remote vulnerability in a VoIP device could subvert all other VoIP security and as a result extensive testing of both VoIP device software and hardware is needed if we are to prevent future intrusions.

During this talk I will outline why the security of the software powering VoIP networks is of critical importance and why businesses, developers and security auditors need to pay more attention to the software they are deploying, developing and testing in real world installations. I will show the need for an automated, black box, protocol compliant and open source testing suite. I will then present VoIPER, a cross platform, easy to use toolkit that can automatically and extensively test VoIP devices as well as providing extensive target management, logging and crash detection critical to modern security testing. VoIPER includes a fuzzing suite which is fully protocol aware and can generate hundreds of thousands of tests for the major VoIP protocols. Unlike many attempts at fuzzing VoIP, VoIPER can interact with the devices under test in a fully protocol compliant fashion and potentially test their entire state spaces.
Its classes are easy to use and extendable to allow users to piece together protocol compliant tests and integrate them with the main test suite.

VoIPER has been used to discover security vulnerabilities in every device tested during its initial testing phase including soft-phones, hard-phones, gateways and servers.

The World of Pager Sniffing/ Interception: More Activity than One May Suspect

NYCMIKE
Hobbyist Signals Collector

Paging networks once sat at the top of the personal and professional communication pyramid. Cell phone technology's have since replaced the now legacy networks at the consumer level, with the exception of niche markets (Due to the signal quality in doors: IT, Emergency Services, Government) the technology may have been retired to a permanent stay in a junk pile. With the fleeing attention and use, it appears that sniffing/interception of pager traffic within the United States has declined to almost a standstill. The scope of this paper is to re-introduce the activity of FLEX (1600/3200 level 2, 3200/6400 level 4) and POCSAG (512, 1200, 2400) then present how a hobbyist can decode it, provide a first hand account of how to install and operate a pager "listening Post", introduce a few ways to use captured cap codes, and offer a conceptual "new" technique in capture pager traffic. With that said, my expertise is limited and I by no means should be considered an expert nor should this writing be interpreted as testament. Last but not least there are laws governing over RF interception and they must be adhered (this means you). Decoding digital data with a soundcard now a days is easier than getting on the internet.

Hacking OpenVMS

Christer Öberg
Security Researcher
Claes Nyberg
Security Researcher
James Tusini
Security Researcher

OpenVMS is considered a highly secure and reliable operating system relied upon by large enterprises around the globe such as Stock Exchanges, Governments and Infrastructure for critical operations. Our talk will focus on subverting the security of the OpenVMS operating system in a number of new and creative ways. There will be an initial brief introduction to the OS basics, security model and its core features. We will also talk about things we perceive as flaws in the security model and weaknesses in the security features provided by OpenVMS. There will also be a practical demonstration of the 0day vulnerabilities found, ranging from logical to memory corruption bugs, along with discussion on how these were found and exploited and obstacles encountered in the process.

Every Breath You Take

Jim O'Leary
Security Researcher

How much data do you generate in the process of living an ordinary day? This talk covers various ways to gather, persist and analyze the data stream that is your life. We'll cover a few of the approaches that are available today, some easy code you can whip up to persist anything you please, and what to expect from the community and businesses moving forward. Privacy/security impact is sure to be huge, so hold on to your hats, and start tracking and logging everything! Somebody else may be doing it for you already..

365-Day: Active Https Cookie Hijacking

Mike Perry
Reverse Engineer, Riverbed Technology

Last year during my Tor presentations at Black Hat and Defcon, and in a follow up post on BugTraq, I announced that many SSL secured websites are vulnerable to cookie hijacking by way of content element injection. Unfortunately, my announcement was overshadowed by Robert Graham's passive cookie stealing attacks (aka 'SideJacking').

The difference between our attacks is this: instead of sniffing passively for cookies, it is possible to actively cull them from targets on your local network by injecting images/iframes for desired sites into unrelated webpages. Moreover, since many sites do not set the 'secure' bit for their SSL cookies, it is even possible to grab cookies used in https sessions and use them to impersonate users. This will be demonstrated.

At the time of this writing, vulnerable SSL sites include Gmail, Facebook, Amazon, and many others. Since wide-spread awareness of the threat seems to be the only way to convince these vendors that they need to secure their cookies, fully automated exploit code will be provided two weeks after the demonstration (however, it is also possible to steal insecure https cookies with just airpwn and wireshark).

Urban Exploration - A Hacker's View

Phreakmonkey
mutantMandias

Urban Exploration is the practice of discovering and exploring (and often photographing) the more "off-beat" areas of human civilization. Popular targets of Urban Exploration include abandoned hospitals or institutions, empty factories, and other disused structures, but it can also include "active" sites such as service corridors, utility levels, rooftops, storm drains, steam tunnels, you name it.

For years, the Urban Exploration community and Hacker community have existed in parallel despite their many commonalities. This talk will introduce UrbEx to the DefCon community and explore the similarity of the mindsets between those who explore the far reaches of cyberspace and those who explore the forgotten areas of the real world.

Bring an open mind, a sense of adventure, and any experiences you've had when you've wandered into a forgotten or "off limits" area just to see what's there. You might already be an Urban Explorer and not have realized it!

Malware Detection through Network Flow Analysis

Bruce Potter
Founder, The Shmoo Group

Over the last several years, we've seen a decrease in effectiveness of "classical" security tools. The nature of the present day attacks is very different from what the security community has been used to in the past. Rather than wide-spread worms and viruses that cause general havoc, attackers are directly targeting their victims in order to achieve monetary or military gain. These attacks are blowing right past firewalls and anti-virus and placing malware deep in the enterprise. Ideally, we could fix this problem at its roots; fixing the software that is making us vulnerable. Unfortunately that's going to take a while, and in the interim security engineers and operators need new, advanced tools that allow deeper visibility into systems and networks while being easy and efficient to use.
This talk will focus on using network flows to detect advanced malware. Network flows, made popular by Cisco's NetFlow implementation available on almost all their routers, has been used for years for network engineering purposes. And while there has been some capability for security analysis against these flows, there has been little interest until recently. This talk will describe NetFlow and how to implement it in your network. It will also examine advanced statistical analysis techniques that make finding malware and attackers easier. I will release a new version of Psyche, an open source flow analysis tool, and show specific examples of how to detect malware on live networks. I will also release a tool designed to craft and spoof netflow records for injection into netflow collectors.

The True Story of the Radioactive Boyscout: The Fwirst Nuclear Hacker and How His Work Relates to Homeland Security's Model of the Dirty Bomb

Paul F. Renda
Data Security Analyst

David Hahn was working on his atomic energy Eagle Scout badge when he had the idea why not build a reactor. However, not just any reactor, he would build a breeder reactor. This type of reactor produces more fuel and power as long as it is working. David used social engineering, unlimited drive and resourcefulness to produce his reactor type device. He succeeded further that any expert in the nuclear world would have dreamed.

Ultimately, the EPA had to clean up his work shed as nuclear and chemical waste site.

I am going to perform a couple of Simple Safe demos related to David's work.

The second part of the talk will deal with Homeland Security's model of the dirty bomb. I will show how David's reactor relates to the current model.
At the end of the talk, I will issue the first annual Dr. Strangelove award for the best question submitted to Me. I have a lot of material to cover so try to study up on reactors.

How can I pwn thee? Let me count the ways

Renderman
Church of WiFi

The wonders of technology have given rise to a new breed of workforce, the mobile workforce. Able to leap large oceans in a single cattle class bound, they are the newest agent of business and the newest pain in your butt. The average business traveler carries with him a multitude of ways to get pwn'd while away from the office and away from your watchful BOFH eye. Come count the ways we can pwn that beleaguered business traveler without even touching him.

10 things that are pissing me off

Renderman
Church of WiFi

This year will be my 10th year of Defcon and my liver has the scars to prove it. In that time I've learned that this community can do anything. In that time I've also become a jaded and bitter IT consultant and there are alot of things pissing me off in the tech world. Some of these things have pissed me off that I'm finally doing something about it, others I need your help. Come get an idea what's in my head pissing me off, and probably pissing you off as well, and what you and I can do about it.

The Big Picture: Digital Cinema Technology and Security

Mike Renlund
Security Researcher

Digital Cinema. Its the first major upgrade to a movie's image in more than 50 years, and it has brought new standards of quality, security, and technology into your local theater complex. This talk will cover what the new BIG PICTURE is all about, the changes made from film, both in the image and sound, and the new security methods involved that help prevent piracy. 3D and alternative content will also be discussed. Come see where the technology stands, and where it is going, and how to get the most out of your movie going experience.

presentations cont.

New Tool for SQL Injection with DNS Exfiltration

Robert Ricks
Senior Information Systems Engineer, G2, Inc.

For years people have been warned that blind SQL injection is a problem, yet there are a multitude of vulnerable websites out there to this day. Perhaps people don't realize that these vulnerabilities are very real. The current state of the art tools are Absinthe and SQL Brute for exploiting blind SQL injection. DNS exfiltration has been proposed as a method of reaching previously unassai able blind SQL injection access points. We have created a proof-of-concept tool which can download an Oracle schema and data from its tables in an automated fashion using DNS as its exfiltration mechanism. Unlike Absinthe this tool does not require any difference between successful and unsuccessful queries to work. It is also much faster than current tools since it can retrieve more than one byte of information at a time and doesn't require noticeable differences in timing. Perhaps this will help people realize that their private data is exceedingly vulnerable if they have even one SQL injection access point and don't take appropriate precautions.

Advanced Physical Attacks: Going Beyond Social Engineering and Dumpster Diving Or, Techniques of Industrial Espionage

Eric Schmiedl
Security Researcher

Your stack is smash-proof. Your dumpster is fully alarmed. And your firewall is so secure that it has former Soviet officials green with envy. So why are the developers finding their undocumented features in competitors' products, or company executives on a constant hunt for leaks and traitors? There's a whole lot more to doing an end-run around network security than calling up and pretending to be the help desk or hoping someone chucks a service manual in the trash Professional attackers with specific targets have a whole rash of techniques — from using targeted employees to hiding microphones — adopted from the world of espionage, and this talk is all about how they do what they do.

Gaming - The Next Overlooked Security Hole

Ferdinand Schober
Security Researcher

"Thanks to Web 2.0 and other over hyped BS, development has been moving farther and farther away from bare metal. Assuming you trust your libraries, this could even be called a good thing. If you're high."

PC gaming, despite Microsoft's best efforts, is not dead. Yet. The modding community is alive and active, and even those same over hyped web technologies are starting to encroach in to shaders, and other things they shouldn't touch. Let's no even get started on the shady communities providing bots, cheats, and other grey market goods.

We're now seeing those unifying technologies the web, and monolithic engines making their way in to these games. Automatic updates, electronic publishing systems, in-game advertisements, pay-for-item MMORPG systems all of these represent structural weaknesses that more and more people should be exploiting. Given the expectation of today's gamers a far as graphics, physics, and other frivolous crap, smaller developers have to purchase someone else's engine to get started and all of the bugs that come with it.

This presentation will begin with a quick overview of what we've seen so far, and will progress in to specific weak points in current and future releases.

High points will include:

- » Why buying someone else's engine is a bad idea (with charts!)
- » The proliferation of middleware, and the homogenization of gaming
- » The little "nude patch" that could: how to own yourself
- » Fake world + real money + ??? = Profit, or the economics of game exploits

Making a Text Adventure Documentary

Jason Scott
Textfiles.com

For the past 3 years, Jason Scott (creator of BBS: The Documentary) has been working on another project, telling the history and the legends of text adventure games. 80 interviews later, he comes to DEFCON to show footage, describe the process of making the film, why history of games is important, and what it was like to visit the actual cave the first adventure game was based on.

Free Anonymous Internet Using Modified Cable Modems

Blake Self
Security Researcher, SERC
Durandal
Vice President, SOLDIERX
Bitemytaco
Co-owner, Surfboard Hacker

Using various modifications and techniques, it is possible to gain free and anonymous cable modem internet access. This talk will analyze and discuss the tools, techniques, and technology behind both hacking cable modems and attempting to catch the users who are hacking cable modems. Previously confidential information gained from a senior network technician at Time Warner will be disclosed in this speech. We will also talk about how these techniques have been used to keep various heavily used servers online and anonymous for over six months without detection.

StegoFS

James Shewmaker
Bluenotch

This talk will reintroduce classic steganographic techniques to use with serializing, watermarking, or stashing your data in the latest Internet meme. Why not let everyone who is forwarding yet another painful nut-shot AFHV clip store your data for you? We will create a simple filesystem that is robust enough to survive conversion, and building a structure to organize the data, focusing on indirection and fault tolerance.

Let's Sink the Phishermen's Boat!

Teo Sze Siong
Security Researcher, F-Secure Corporation
Hirosh Joseph
Security Researcher, F-Secure Corporation

In this presentation, an advanced form of phishing attack will be discussed to show the risk how criminals might steal the entire fund from an online banking account protected with daily transaction limit and bypassing the 2-factor authentication system. This type of attack is able to work in stealthy mode without showing theft symptoms in the bank account balance to keep the victims in the dark. Challenges and limitations encountered by the existing phishing detection techniques will be also identified and reviewed to understand the applicability of each technique in different scenarios.

As a step taken to combat phishing attacks effectively, the concept of 'website appearance signature' will be presented and explained how this new concept can be applied to detect unknown phishing websites. This has been a great challenge in the past since most phishing website detection tools verify the reputation of a website using a database of blacklisted URLs. In addition, a Proof-Of-Concept application employing the 'website appearance signature' combining with conventional phishing detection techniques will be demonstrated to see its accuracy and effectiveness as a phishing website detection tool.

Medical Identity Theft

Eric Smith
Assistant Director of Information Security and Networking, Bucknell University
Dr. Shana Dardan
Assistant Professor of Information Systems, Susquehanna University

In less than an hour, during a scheduled pentest, our team was able to retrieve 3.2 million patient insurance records from a HIPAA-compliant medical facility. Using these records, we could have generated counterfeit insurance and prescription cards which would pass muster at any doctor's office or pharmacy counter. If you are one of the 47 million Americans with no health insurance or happen to have a medical condition you wished to hide from employers or insurers, would you consider purchasing falsified medical documents? Thousands of Americans have already said yes, without thinking twice about the victim of their victimless crime.

What happens to you if your medical identity is stolen? You may find yourself liable for thousands of dollars of co-pays, deductibles, and denied claims. Is this because you forgot to shred an important document? Did you fall for a phishing scheme online? Of course not — it was entirely outside of your control, and it happened because the current HIPAA regulations are insufficient to protect your medical identity.

In this talk, we'll review the current state of HIPAA and other laws covering the security of your medical records, and discuss what changes need to be made, both in policy in practice, to shore up the security of our medical records.

CAPTCHAs: Are they really hopeless? (Yes)

Mike Spindel
Security Researcher
Scott Torborg
Web Application Developer

CAPTCHAs are widely used to protect websites against malicious robots. Yet, CAPTCHAs are being broken routinely by spammers, malware authors, and other nefarious characters. This talk will review and demonstrate many of the implementation weaknesses that are routinely exploited to break image-based CAPTCHAs, and offer suggestions for improving the effectiveness of CAPTCHAs. Rather than attempt an in-depth examination of any single CAPTCHA or technique, we will present a broad overview of tools with the aim of making it easy for anyone to take a shot at cracking the CAPTCHAs on present and future high-profile sites.

Living in the RIA World

Alex Stamos
Founding Partner, iSEC Partners Inc.
David Thiel
Senior Security Consultant, iSEC Partners
Justine Osborne
Security Consultant, iSEC Partners

Rich Internet Applications (RIA) represent the next generation of the Web. Designed to run without constant Internet connectivity, they provide a graphical experience equivalent to thick desktop applications with the easy install experience of thin Web apps. They intentionally blur the line between websites and traditional desktop applications and greatly complicate the jobs of web developers, corporate security teams, and external security professionals.
Our goal with this talk will be to outline the different attack scenarios that exist in the RIA world and to provide a comparison between the security models of the leading RIA platforms. We will discuss how current attacks against web applications are changed with RIA as well as outline new types of vulnerabilities that are unique to this paradigm. Attendees will learn how to analyze the threat posed to them by RIA applications as either providers or consumers of software built on these new platforms.

We will also be discussing the attack surface exposed by the large media codec stacks contained in each of these platforms. Our targeted platforms include Adobe AIR, Microsoft Silverlight, Google Gears, JavaFX, and Mozilla Prism. At this talk, we will be releasing tools for testing the codec security of these platforms as well as sample malicious code demonstrating the danger of RIA applications.

Xploiting Google Gadgets: Gmalware and Beyond

Tom "strace" Stracener
Senior Security Analyst
Robert "Rsnake" Hansen
CEO SecTheory

Google Gadgets are symptomatic of the Way 2.0 Way of things: from lame gadgets that rotate through pictures of puppies to calendars, and inline email on your iGoogle homepage. This talk will analyze the security history of Google Gadgets and demonstrate ways to exploit Gadgets for nefarious purposes. We will also show ways to create Gadgets that allow you to port scan internal systems and do various JavaScript hacks via malicious (or useful) gadgets, depending on your point of view. We've already ported various JavaScript attack utilities to Google Gadgets (like PDP's JavaScript port scanner) among other things. We will also disclose a zero day vulnerability in Google Gadgets that makes Gmalware (Gmodules based malware) a significant threat.

Inducing Momentary Faults Within Secure Smartcards / Microcontrollers

Christopher Tarnovsky
Flylogic Engineering, LLC

This presentation is intended for individuals with an understanding of the Intel 8051 and Motorola 6805 processor families from an Assembly language perspective. This will be an interactive presentation with the audience.

Log files will be examined that have been taken from the targets (smartcards) at every clock cycle of the CPU during its runtime. We will discuss our possibilities and determine points in time (clock cycle periods) to momentarily induce a fault within the target.

Our goal will be to override the normal behavior of the target for our own use such as:

- » Temporary changes – Readout of normally private records from the device
- » Permanent changes – Change non-volatile memory to create a back-door or completely rewrite behavior model

Both smartcards contain a Cryptographic co-processor and are known to have been used to secure Data, PCs, laptops and Sun-Ray terminals.

Open in 30 Seconds: Cracking One of the Most Secure Locks in America

Marc Weber Tobias
Investigative Attorney and Security Specialist – Security.org
Matt Fiddler
Security Specialist – Security.org

Many high security lock manufacturers claim that their cylinders are impervious to covert methods of entry including picking, bumping, and decoding and that they offer high levels of key control, effectively preventing the illegal or unauthorized duplication of their keys. New and unique methods to compromise one of the most secure locks in America by forced, covert, and surreptitious entry were developed during an eighteen month research project that has resulted in the filing of multiple patents and the ability to pick, bump, and mechanically bypass Medeco cylinders, sometimes in seconds. In this presentation we offer a detailed analysis of how the Medeco lock was compromised by a methodical analysis of its physical characteristics and their code database.
Medeco is the dominant leader in the North American high security lock sector. They protect venues that include the White House, Pentagon, and Royal Family residence in London. They are relied upon throughout the world for their security and invulnerability to attacks. As a result of disclosures by the presenters at DEFCON 15, they were forced to urgently upgrade their deadbolt locks. The new techniques of bypass that will be disclosed in this presentation will be equally significant, if not even more concerning because of their widespread security implications.

Hijacking the Outdoor Digital Billboard Network

Tottenkoph
Business Analyst, Raymond James Financial
Rev
Security Researcher
Philosopher
Security Researcher

Outdoor digital billboards are becoming the new way to advertise multiple products/services/etc with a single board as compared to having a street littered with dozens of these eyesores. Therefore, they're more fun to take apart and play with. While driving one day, I noticed a 404 error on one of these billboards and after discussing it with my fellow speakers, hatched a plan to hack into their network and advertise our own ideas/ "products". We will be talking about how we exploited the physical and network security of this well known company and used these to upload our own images. This is *not* a step-by-step how to, but rather addresses the vulnerabilities that exist and how they could be used for guerilla advertising and digital graffiti.

How to make Friends & Influence Lock Manufacturers

Schuyler Towne
Executive Editor, Non-Destructive Entry Magazine
Jon King
Inventor, Medecoder

Locksport is growing up in America. In this talk we will explore four case studies demonstrating how the community has leveraged itself to bring about significant advances in the lock industry. We will demonstrate exploits discovered in both Medeco and ABUS high security locks and discuss how Kwikset's Smartkey system responded to the spread of information about bumping and how they plan to work with the community in the future. We will investigate the Robo-Key System, a new lock that has been developed in an open source atmosphere alongside the locksport community. Finally, a plea to the hacker community to help us continue the work we've started researching locking systems as more move into the electronic and digital realms and fostering positive relationships with the manufacturers.

Evade IDS/IPS Systems using Geospatial Threat Detection

Ryan Trost
Director of Security, Comprehensive Health Services

IDS/IPS systems are becoming more and more advanced and geocoding is adding another layer of intelligence to try and defend against a company's vulnerabilities. Learn how to evade complex geospatial threat detection countermeasures. Most crackers use zombie machines to launch professional attacks...but zombies even leave geographic fingerprints that are easily picked up by pattern recognition algorithms. Learn how to take professional attacks to the next level.

MetaPost-Exploitation

Valsmith
CTO, Offensive Computing, LLC
Colin Ames
Researcher, Offensive Computing, LLC

When penetration testing large environments, testers require the ability to maintain persistent access to systems they have exploited, leverage trusts to access other systems, and increase their foothold into the target. Post exploitation activities are some of the most labor intensive aspects of pen testing. These include password management, persistent host access, privileged escalation, trust relationships, acquiring GUI access, etc. Penetration testers acquire hashes, crack them, keep track of which passwords go with which usernames / systems and finally reuse this information to penetrate further systems.

Keeping Secret Secrets Secret and Sharing Secret Secrets Secretly

Vic Vandal
504 / NOLAB / NC2600

Have you ever wanted to:

- » Transmit secret codes and messages
- » Protect Nuclear launch codes
- » Dabble in Intellectual Property protection
- » Warez/file-sharing with legal liability protection
- » Develop and share terrorist plots
- » Smuggle illegal substances
- » Hide digital pr0n from others
- » Exchange classified information securely
- » Exchange diskette with "Leonardo da Vinci" virus, culled from the hacked "garbage" file on the Gibson
- » ???

If you answered "YES" to any of these questions then this talk is for you. Vic will walk you through the shadowy world of secret-splitting, steganography, spy tactics, and other methods to hide and/or exchange sensitive materials and information — without the use of traditional cryptography. Both digital and physical protection schemes will be covered during the course of the presentation. The audience will also get to play along in a handful of online challenges. So gird your loins, lock up your women and children, put on your dark sunglasses, and come join the fun.

For those interested in playing along during the stego portion of the talk, consider pre-installing any/all of the following tools:

- » GiftItUp (Windows)
- » S-Tools (Windows)
- » JPHS (Windows)
- » MP3Stego (Windows or Linux)
- » Camouflage (Windows)
- » Stego (Mac)
- » Hydan (Linux)

Compliance: The Enterprise Vulnerability Roadmap

Weasel
Nomad Mobile Research Centre

Compliance is no longer new. Compliance has been accepted by the corporate-state. Compliance is common-place. Compliance is the intruders' new friend. Decision makers thinks Compliance == Security. While many compliance standards have resulted in the implementation of some very important controls, they have also left a roadmap for intruders, ill doers and the sort to hone their attack. This presentation will go over such weaknesses and show how compliance entities are, regardless of intent, proving that compliance != security.

presentations cont.

Password Cracking on a Budget

Matt Weir
Security Researcher
Sudhir Aggarwal
Security Researcher

Not every bad guy writes down passwords on sticky note by their monitor. Not every system administrator fully documents everything before they leave. There are a lot of legitimate reasons why you might need to crack a password. The problem is most people don't have a supercomputer sitting in their basement or the money to go out and buy a rack of FPGAs. This talk deals with getting the most out of the computing resources you do have when cracking passwords.

In this talk, we'll go over some of the tools and techniques we've used to crack these password lists using only a couple of PCs, such as custom wordlist generation and choosing the right word mangling rules. We'll also talk about some of the lessons we've learned and the mistakes we've made along the way.

RE:Trace: The Reverse Engineer's Unexpected Swiss Army Knife

David Weston
Security Engineer, SAIC
Tiller Beauchamp
Senior Security Engineer, SAIC

This presentation will detail the newest developments in RE:Trace, a reverse engineering framework based on Ruby and DTrace. We will discuss implementations for walking and searching the heap on OS X, tracing for kernel and driver vulnerabilities, pinpointing format string bugs and leveraging custom application probes, such as those built into browser and database software.

Mobile Hacker Space

Thomas Wilhelm
Founder, De-ICE.net

There has been a recent global push for the creation of Hacker Spaces. Unfortunately, these ventures are risky and can be quite costly. In an effort to provide an alternative, or at least an intermediary step, this talk will discuss a different type of Hacker Space, one that is on wheels. During the course of this speech, we will discuss the advantages and disadvantages of building a mobile hacker space, and present a real-world example, which will be open to tours at DefCon (as long as it doesn't break down before it gets there). We will talk about the problems and solutions associated with the development of a mobile hacker space, and offer ideas for future designs. In addition, a list of current and future hacker projects will be discussed, and include IT-related and vehicle-related hacks.

Web Privacy and Flash Local Shared Objects

Clinton Wong
Security Researcher

This talk discusses privacy issues concerning Adobe Flash Local Shared Objects. Adobe LSOs are similar to HTTP cookies, but not as easily controlled or configured using a standard web browser. Potential problems with Flash LSOs will be presented, as well as suggestions for increasing privacy while using Adobe LSOs.

New ideas for old practices - Port-Scanning improved

Fabian "fabs" Yamaguchi
Recurity Labs GmbH, Berlin, Germany
FX
Head of Recurity Labs

How fast a port-scan can be is largely dependent on the performance of the network in question. Nonetheless, it is clear that choosing the most efficient scanning-speed is only possible based on sufficient information on the network's performance. We have thus designed and implemented a port-scanning method which provokes extra network-activity to increase the amount of information at our disposal in an attempt to gain speed on the long run.

Following this approach, we've managed to mimic TCPs properties to an extend which allows us to implement many congestion control schemes initially designed for TCP. Further tweaking the actual implementation by integrating it into the linux-kernel left us with a port-scanner ready to tackle big networks at an impressive speed.

The Death Envelope: A Medieval Solution to a 21st Century Problem

Matt Yoder
Security Researcher

While many aftercare solutions and recommendations cover "average American" needs, none have tackled, full-on, the needs of the rapidly growing high tech segment of the population. As the amount of passwords and other secret "brainspace-only" information grows for many, many, individuals, it becomes obvious that a solution is needed for the dispensation of this information in the event of one's death or extreme disablement. It turns out that this solution may be the humble paper envelope.

This talk begins to examine an approach to handle this problem, offering many suggestions, from the extremely reliable low-tech end, through hybrid and high tech solutions to the problem. It covers, as well, recommendations for what to include in one's envelope, and how to ensure its safety, security, and integrity. It also discusses why a wax stamp, sealed by a signet ring, no less, may still offer the best envelope tamper detection that exists.

Panel: All Your Sploits (and Servers) Are Belong To Us: Vulnerabilities Don't Matter (And Neither Does Your Security)

David Mortman
CSO in Residence, Echelon One
Rich Mogull
Securosis
Chris Hoff
Unisys
Robert "RSnake" Hansen
CTO, SecTheory
Robert Graham
CTO, Errata Security
David Maynor
CTO, Errata Security

Think that latest buffer overflow or XSS exploit matters? It doesn't. Think your network is secure because you have the latest and greatest IPS? It isn't. The truth is all exploits or defenses on their own are worthless; it's how you use your tools and respond to incidents that really matters. This panel, composed of top vulnerability and security researchers, will roll through a rapid-fire series of demonstrations as they smash through the security of popular consumer and enterprise devices and systems, often using simple techniques rather than the latest 0day exploits (but we'll see a few of those too). They'll then debate the value of any single attack vector or defense, and show how it's the practical application of attacks, defenses, and (more importantly) responses that really matters. From iPhones to browsers to SCADA, it isn't your advanced attack or defensive tool that matters, it's what you do with it.

Panel: Black vs. White: The complete life cycle of a real world breach

David Kennedy
Practice Lead: Profiling & e.Discovery, SecureState
Ken Stasiak
President & CEO, SecureState
Scott White
Senior Security Consultant, SecureState
John Melvin
Senior Security Consultant, SecureState
Andrew Weidenhamer
Staff Security Consultant, SecureState

Black vs. White: The complete life cycle of a real world breach combines a unique idea and a real-world case study from a client of ours that details the start of a hack to the identification, forensics, and reversing. We will be discussing some advanced penetration techniques and reversing topics. Starting off, we will be performing a full system compromise from the internet (complete with live demos), installing some undetectable viruses, and having a separate team reverse it, and show you what its doing and how it works. This is the ultimate battle of evil verses good.

Additionally, what would a con be without some awesome tool releases? We will be releasing (and demoing) two tools, one a Windows GUI for the windows folks that does everything for SQL injection rooting, minus making you breakfast, one Linux based tool that auto crawls a site and performs blind/error based SQL injection with reverse command shells using various options for payload delivery.

Panel: Hacking in the Name of Science

Tadayoshi Kohno
Assistant Professor, University of Washington
Jon Callas
Chief Technology Officer, PGP Corporation
Alexei Czeskis
PhD Student, University of Washington
Dan Halperin
PhD Student, University of Washington
Karl Koscher
PhD Student, University of Washington
Michael Piatek
PhD Student, University of Washington

Our talk will start with some of our latest and greatest hacks. In 2003 we were the first to analyze the security of Diebold's AccuVote-TS voting machine software. We'll discuss the inside scoop on how we got the code, broke it, and then went public. In 2008 we also published the first attacks against a real, common wireless implantable medical device – an implantable defibrillator and pacemaker – and we did so using off-the-shelf software radios. What else will we talk about? Well, there was our research in measuring just how frequently ISPs are injecting ads into people's web pages, our framing of network printers for copyright infringement (and receiving DMCA takedown notices to those printers), our invention of clock skew-based remote physical device fingerprinting, and much more.

Are we hackers? No, we're scientists at a leading public university. So what turns hacking into "science" when it's done by academics? We'll answer these and other questions in the second half of the talk, which is geared to give you an inside glimpse into the world of academic security research. Along the way we'll answer questions like: How do we choose which technologies to hack–or as we say– "analyze," "study," and "investigate?" What might we hack next? What can we do as academic researchers in public institutions that industry researchers can't? What ethical and legal issues do we need to consider? And why is what we do considered "science?" Anyone who doesn't want their product to be the next technology hacked (sorry, "studied") by academics like us should definitely attend this talk. And, of course, come to this talk if you're considering grad school in computer security. We'll also debate how academics and industry security researchers could better work together. Here we'd particularly like your feedback. What can academics learn from you? What do you think we could do better? What would you like us to look at next?

(Standard academic disclaimer: Many of the works will discuss were previously published in conjunction with other researchers. We'll acknowledge all relevant parties in the talk.)

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

Kevin Bankston
Senior Staff Attorney, EFF
Eva Galperin
Referral Coordinator, EFF
Jennifer Granick
Civil Liberties Director, EFF
Marcia Hofmann
Staff Attorney, EFF
Corynne McSherry
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 NSA wiretapping and fighting efforts to use intellectual property claims to shut down free speech and halt innovation, highlighting our open government efforts with documents obtained through the Freedom of Information Act on government surveillance efforts, introducing the Coder's Rights Project, and much more. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.

Panel: Internet Wars 2008

This year's panel members will be announced closer to the conference date.

Continuing our new tradition from the past two years, leading experts from different industries, academia and law enforcement will go on stage and participate in this panel, discussing the current threats on and to the Internet, from regular cyber-crime all the way to the mafia, and even some information warfare.

In this panel session we will begin with a short (2-5 minutes) introductory presentation from Gadi Evron on the latest technologies and operations by the Bad Guys and the Good Guys. What's going on with Internet operations, global routing, botnets, extortion, phishing and the annual revenue the mafia is getting from it. The members will accept questions on any subject related to the topic at hand, and 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 is to be limited to issues happening on the Internet, rather than this or that vulnerability. The discussion is mostly technological and operational in nature, although for example two years ago attendees chose to ask questions directing the discussion to the legal side of things. Participants are people who are involved with battling cyber-crime daily, and are some of the leaders in the security operations community of the Internet.

Panel: Meet the Feds 2008

Jim Christy
DC3
Randy Duvay
NCIS
James Finch
FBI
Barry Grundy
NASA
Bob Hopper
NW3C
Ray Kessenich
DCITA
Tim Kosiba
NSA
Mischel Kwon
USCERT
Rich Marshall
NSA
Tom Pownall
RCMP
Ken Privette
USPS IG
Lin Wells
NDU

Ever had to sweat through an interrogation or watch some poor sap suffer a similar fate? Have you ever wanted to turn the tables and put those cruel individuals responsible on the chopping block? Well, now you can! With representatives from NSA, NASA, FBI, IRS, DHS, and other fine Federal agencies, you will have an abundance of opportunities to attempt to humiliate, harass, threaten, or even bring them to tears. Go ahead hack away and take your best shot! Remember, what is said on this panel in Vegas, stays on this panel in Vegas...

Again this year we will have many federal agencies -

Information Assurance Panel: CERTS, first responder's organizations from agencies including DC3, DHS USCERT, NSA, OSD, and NDU

Law Enforcement Counterintelligence Panel: including DC3, FBI, IRS, NCIS, NASA, NWC3, US Postal IG

Each of the agency reps make an opening statement regarding their agencies role, then open it up to the audience for questions.

Agencies that will have representatives include: Defense Cyber Crime Center (DC3), FBI, IRS, NCIS, NASA, DHS USCERT, DoJ, National White Collar Crime Center (NWC3), NSA, US Postal IG, Office of the Secretary of Defense, National Defense University.

For years Defcon participants have played "Spot the Fed." For the 3rd year, the feds will play "Spot the Lamer". Come out and nominate a Lamer and watch the feds burn'em.

network @ dc16

WiFi Connections

802.11b/g – DefCon
802.11a – DefConA

The usual network access this year. We've beefed up our back-end this year, working on continued bandwidth and stability (got fiber?). Internet access will be available throughout the entire convention facility (all speaking rooms, CTF, Vendors, Contest area, side-rooms).

We doubled our bandwidth to a guaranteed 20Mb this year! Plenty for everyone, their mom, their dog, AND the kitchen sink.

Many, many thanks to the Network/IT crew that makes this happen every year! We meet up throughout the year at other cons or random travel events to make sure all this happens. Shouts out to Videoman(9 yrs), Heather(8 yrs), effffn (4yrs), Sparky (3yrs), Derek (who couldn't make it this year), Major Malfunction (666 yrs), and our two n00bs this year, Mac and KidKaos!

Cheers!

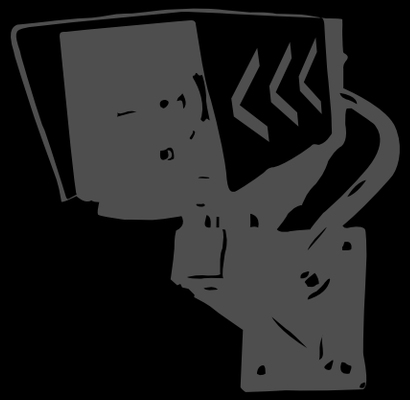
Lockheed
(noc@defconnetworking.org)

Remember to check out http://www.defconnetworking.org/ for post-con stats & wrap-up.

DCTV @ DefCon

This year we're pushing ahead with an experiment we started last year – community-driven DCTV! We've dubbed it MeTooTube. While at the convention, goto http://dctv.defcon.org to check out and upload content to the community. We'll have it running on displays around the convention area.

Feedback & comments -> dctv@defconnetworking.org



Vendors

The Electronic Frontier Foundation (EFF) is the leading organization defending civil liberties in the digital world. We defend free speech on the Internet, fight illegal surveillance, 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.

Flat Nine Studios, LLC is a full service digital media production services company centered in the heart of downtown Orlando, Fl. The company is excited to attend the 2008 Def Con 16 conference in association with Managed Mischief, Inc. to support and celebrate the release of the film Hackers Are People Too. Stop by the Flat Nine Studios vendor booth to meet the crew, pick up your official Flat Nine Studios swag and pick up a copy of the Hackers Are People Too DVD featuring music composed/produced by founding members, Daniel Wilkerson and Lance Kamphaus.

Ghetto Geeks

If Justin was bringing sexy back, then we are most definitely bringing back cyberpunk. A state where right and wrong are subjective terms. Where we will only be able to change, what we want, as long as there's the fiercest tenacity to change it. Stop on by and take a look at the attitude we have and how far we are willing to go to make use of it.

Greensector focuses on the artistic side of our culture. Stop by our booth for unique limited-run t-shirts designs, current DJ mixes, stickers, buttons + other nick-hacks!

Immunity sells professional hacking software and will be offering free Network Offense Professional (NOP) certification exams.

Irvine Underground

Celebrating 7 years of computer security and hacking in Orange County, California. Docendo Discimus - IrvineUnderground.org HackerStickers.com What started with 8 sticker designs and one t-shirt has grown into a whole lifestyle, stop by the booth or visit hackerstickers.com

MECO is selling Rugged laptops, electronic surveillance equipment, military surplus, comsec equipment, and who know's what else...

No Starch Press (nostarch.com), publisher of best-sellers like Hacking: The Art of Exploitation, Hacking the Xbox, Steal This Computer Book, and Silence on the Wire, is offering DEF CON attendees 30% off everything. Spend over $30 and get a free Wacky Package. Buy 2 books and get a shot glass (while they last). Maybe we'll even have t-shirts. Come by, meet us, and buy us a drink.

Simple-WiFi.com

Simple-WiFi is an antenna manufacturer and wireless card reseller of the highest quality products. Simple-WiFi encompasses an advanced engineering staff for custom solutions and bulk pricing. All solutions are tested in a state-of-the-art lab in Miami, Florida. Simple-WiFi antennas are made in the USA.

The University of Advancing Technology (UAT) is a private college in Tempe, AZ created especially for the technophiles of the world. With an existing on-campus population of over 1,000 students and an online community of approximately 250, UAT's resilience in nurturing our community is met with unparalleled fervor. Our geek-centric student population is taught to be innovators of the future through the wielding and manipulation of technology. UAT offers accredited degrees with majors in Network Security, Computer Forensics, Information Security, Artificial Life Programming, Software Engineering, Robotics and Embedded Systems and many others.

BOOK SIGNINGS

Michael Brooks
author of
"13 Things That Don't Make Sense: The Most Baffling Scientific Mysteries of Our Time"
8-Aug 11:30

Marc Weber Tobias
author of
"OPEN IN THIRTY SECONDS: Cracking One of the Most Secure Locks in America"
8-Aug 15:15

at breakpoint Books & More

schedule

DAY 1: Friday, August 8

Time	Track 1	Track 2	Track 3	Track 4	Track 5
10:00-10:50	**Welcome by DT & Making the DEFCON 16 Badge with Joe "Kingpin" Grand**	**Weasel** Compliance: The Enterprise Vulnerablity Roadmap	**Chema Alonso & Jose Parada** Time-Based Blind SQL Injections Using Heavy Queries: A Practical Approach to MS SQL Server, MS Acess, Oracle, MySQL Databases and Marathon Tool.	**Brenno J.S.A de Winter** Hacking Data Retention: Small Sister your Digital Privacy Self Defense.	**Ben Feinstein** The Wide World of WAFs
11:00-11:20	**Schuyler Towne** How to make friends & influence Lock Manufacturers.	**Michael Brooks** Deciphering Captcha	**Ian Angell** Digital Security: A Risky Business	**Joe Cicero** Hacking E.S.P.	**Panel:** Hacking in the Name of Science.
11:30-11:50		**Kolisar** Whitespace: A Different Approach to JavaScript Obfuscation.		**Clinton Wong** Web Privacy & Flash Local Shared Objects.	
12:00-12:50		**Mike Spindel** Captchas: Are they really Hopeless? (Yes!)	**Mark Bristow** ModScan: A SCADA MODBUS Network Scanner	**Roger Dingledine** Security and anonymity vulnerabilities in Tor: past, present, and future	
13:00-13:20	**Marc Weber Tobias** Open in 30 Seconds: Cracking One of the Most Secure Locks in America.	**Tom "Strace" Stracener & Robert "RSnake" Hansen** Xploiting Google Gadgets: Gmalware & Beyond	**Robert Ricks** New Tool for SQL Injection with DNS Exfiltration.	**Jim O'Leary** Every Breath you Take.	**Greg Conti** Could Googling Take Down a President, Prime Minister, or an Average Citizen?
13:30-13:50			**Morgan Marquis-Boire** Fear, Uncertainty and the Digital Armageddon		
14:00-14:50		**Nathan Hamiel & Shawn Moyer** Satan is on my friends list: Attacking Social Networks.	**Kurt Grutzmacher** Nail the Coffin Shut,NTLM is Dead.	**Magnus Bråding** Generic, Decentralized, Unstoppable Anonymity: The Phantom Protocol.	**Jan Newger** Anti-RE Techniques in DRM Code
15:00-15:50	**Eric Schmiedl** Advanced Physical Attacks: Going Beyond Social Engineering and Dumpster Diving Or, Techniques of Industrial Espionage	**Wendel Guglielmetti Henrique** Playing with Web Application Firewalls.	**Kevin Figueroa, Marco Figueroa, & Anthony L. Williams** VLANs Layer 2 Attacks: Their Relevance and their Kryptonite.		**Alex Stamos, David Thiel & Justine Osborne** Living in the RIA World
16:00-16:50	**David Maynor & Robert Graham** Bringing Sexy Back: Breaking in with Style.	**Fyodor** NMAP-Scanning the Internet.	**James Shewmaker** StegoFS	**Blake Self & Durandal** Free Anonymous Internet Using Modified Cable Modems.	**Travis Goodspeed** Journey to the center of the HP28.
17:00 - 17:50	**Matt Yoder** Death Envelope: Medieval Solution to a 21st Century Problem.	**Ben Feinstein** Snort Plug-in Development: Teaching an Old Pig New Tricks.	**D.J. Capelis** Building a Real Session Layer.	**Vic Vandal** Keeping Secret Secrets Secret & Sharing Secret Secrets Secretly.	**Panel:** Meet the Feds
18:00 - 18:50	**Fabian "Fabs" Yamaguchi & FX** New Ideas for Old Practices-Port Scanning Improved.	**Guy Martin** Sniffing Cable Modems.	**John Fitzpatrick** Virtually Hacking.	**Eric Smith & Dr. Shana Dardan** Medical Identity Theft	
19:00 - 19:20				**Nathan Evans** De-TOR-iorate Anonymity	

DAY 2: Saturday, August 9

Time	Track 1	Track 2	Track 3	Track 4	Track 5
10:00 - 10:50	**David Weston & Tiller Beauchamp** RE:Trace: The Reverse Engineer's Unexpected Swiss Army Knife	**Nelson Murilo & Luiz "ef-fffn" Eduardo** Beholder: New WiFi Monitor Tool	**Don Blumenthal** Working With Law Enforcement	**Joe "kingpin" Grand & Zoz** BSODomizer	**G.Mark Hardy- A Hacker Looks at 50**
11:00 - 11:50	**Matt Weir & Suhir Aggarwal** Password Cracking on a Budget	**Thomas d'Otreppe de Bouvette "Mister X" & Rick Farina "Zero_Chaos"** Shifting the Focus of WiFi Security: Beyond Cracking your neighbor's WEP key	**Scott Moulton** Forensics is ONLY for Private Investigators	**Cameron Hotchkies** Under the iHood	**Ferdinand Schober** Gaming- The Next Overlooked Security Hole
12:00 - 12:50	**FX** Developments in Cisco IOS Forensics	**Matt "DCFLuX" Krick** Flux on:EAS (Emergency Alert System)	**John "Jur1st" Benson** When Lawyers Attack! Dealing with the New Rules of Electronic Discovery	**Jay Beale** Owning the Users with Agent in the Middle	**NeOnRa1n & Joe "Kingpin" Grand** Brain Games: Make your own Biofeedback Video Game
13:00 - 13:50	**Adam Bregenzer** Buying Time- What is your Data Worth? (A Generalized Solution to Distributed Brute Force Attacks)	**Alexander Lash** Taking Back your Cellphone		**Luciano Bello & Maximiliano Bertacchini** Predictable RNG in the Vulnerable Debian OpenSSL Package, the What and the How	**Ian Clarke** Hacking Desire
14:00 - 14:50	**Panel:** All your Sploits (and Servers) are belong to us	**Major Malfunction** Feed my SAT Monkey	**Panel:** Ask the EFF The Year in Digital Civil Liberties Panel	**SensePost** Pushing the Camel through the eye of a needle	**Lyn** Tuning Your Brain
15:00 - 15:50		**Zac Franken** Is that a unique credential in your pocket or are you just pleased to see me?		**Mati Aharoni** BackTrack Foo- From bug to 0day	**Phreakmonkey & mutant-Mandias** Urban Exploration- A Hacker's View
16:00 - 16:20	**Michael Brooks** CSRF Bouncing	**Mike Perry** 365-Day:Active https cookie hijacking	**Panel:** Commission on Cyber Security for the 44th Presidency	**atlas** VulnCatcher: Fun with Vtrace & Programmatic Debugging	**Lee Kushner & Mike Murray** Career Mythbusters: Separating Fact from Fiction in your Information Security Career
16:30 - 16:50		**MD Sohail Ahmad,JVR Murthy & Amit Vartak** Autoimmunity Disorder in Wireless LANs			
17:00 - 17:20	**To Be Announced**	**NYCMIKE** The World of Pager Sniffing/ Interception: More Activity than one may suspect	**Don Blumenthal** What to do when your Data winds up where it shouldn't	**David Byrne** Grendel-Scan: A New Web Application Scanning Tool	**Christopher Tarnovsky** Introducing Momentary Faults Within Secure Smartcards/ Microcontrollers
17:20 - 17:50		**Fouad Kiamilev & Ryan Hoover** Demonstration of Hardware Trojans			
18:00 - 18:50	**Paul F. Renda** The True Story of the Radioactive Boyscout: The first Nuclear Hacker & how his work relates to Homeland Security's model of the dirty bomb	**Scott Moulton** Solid State Drives Destroy Forensic & Data Recovery Jobs: Animated!	**To Be Announced**	**Renderman** How can I pwn thee? Let me count the ways	

schedule

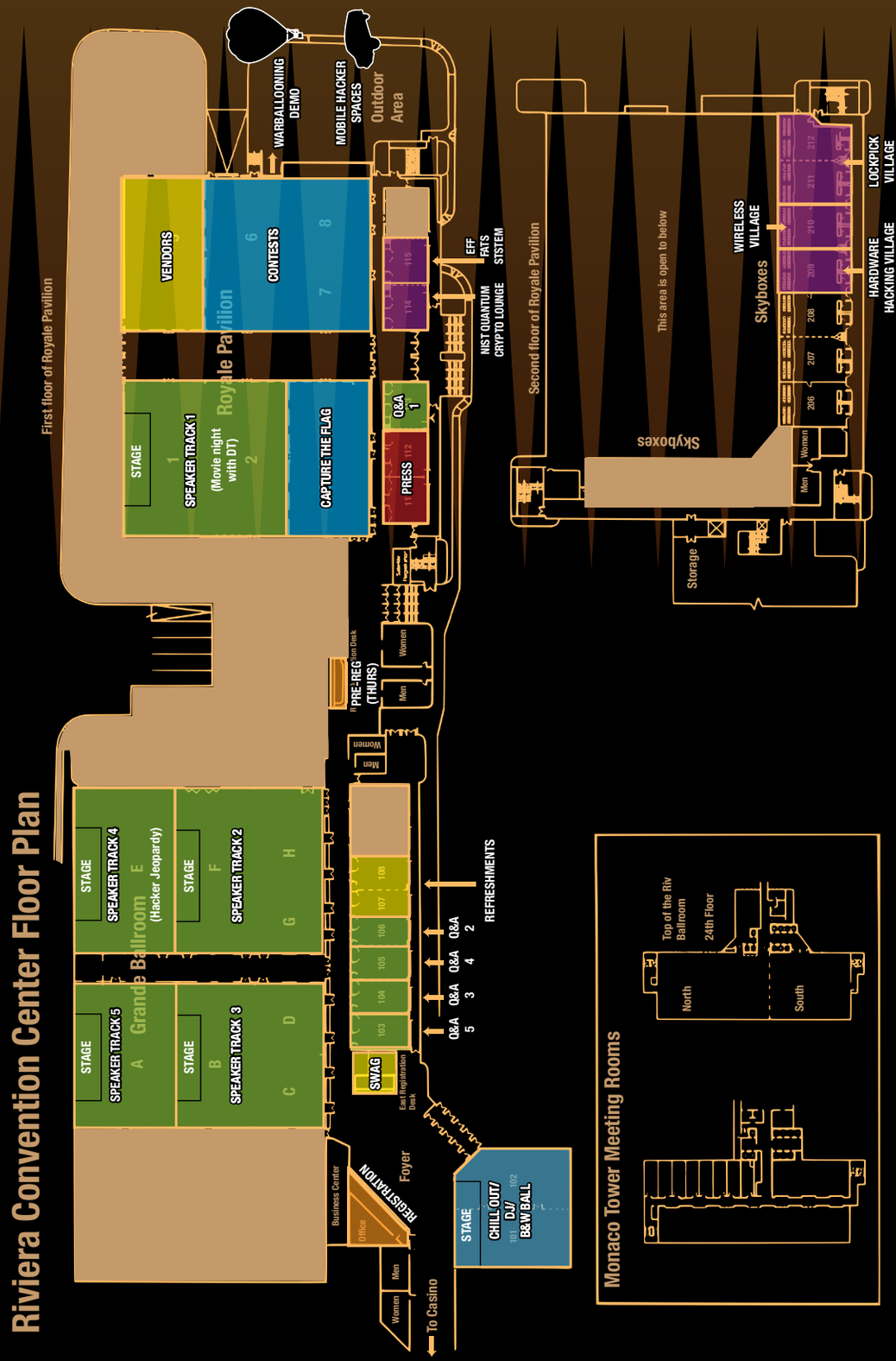
DAY 3: Sunday, August 10

Time	Track 1	Track 2	Track 3	Track 4	Track 5
10:00-10:20	**Bruce Potter** Malware Detection through Network Flow Analysis.	**Brian K. Edwards** Markets for Malware: A Structural Economic Approach	**Tony Howlett** The death of Cash: The Loss of anonymity & other danger of the cash free society.	**Christer Oberg, Claes Nyberg, & James Tusini** Hacking Open VMS.	**Stefan Frei, Thomas Duebendorfer, Gunter Ollman & Martin May** Exploiting A Hundred-Million Hosts Before Brunch
10:30 - 10:50		**Ryan Trost** Evade IDS/IPS Systems using Geospatial Threat Detection.	**Peter Berghammer** The Emergence (and use) of Open Source Warfare.		**JonM** Ham for Hackers-Take back the Airwaves.
11:00 - 11:50	**Rick Hill** War Ballooning-Kismet Wireless "Eye in the Sky"	**Dan Kaminsky** TBA	**Sandy Clark "Mouse"** Climbing Everest: An Insider's Look at one state's Voting Systems.	**N.N.P.** VoIPER:Smashing the VoIP Stack while you sleep.	**Nick Harbour** Advanced Software Armoring and Polymorphic Kung Fu
12:00 - 12:20	**Simon Howard** Race-2-Zero Unpacked	**Teo Sze Siong & Hirosh Joseph** Let's Sink the Phishermen's Boat!	**Doug Farre** Identification Card Security: Past, Present, Future.	**Jay Beale** They're Hacking Our Clients! Introducing Free Client-side Intrustion Prevention.	**Valsmith & Colin Ames** MetaPost-Exploitation
12:30 - 12:50		**Renderman** 10 Things that are Pissing me off			
13:00 - 13:50	**Thomas Wilhelm** Mobile Hacker Space	**Anthony Martinez & Thomas Bowen** Toasterkit, a Modular NetBSD Rootkit	**Zack Anderson, RJ Ryan & Alessandro Chiesa** The Anatomy of a Subway Hack: Breaking Crypto RFID's & Magstripes of Ticketing Systems	**Paul Craig** Compromising Windows Based Internet Kiosks.	**Jonathan Brossard** Bypassing pre-boot authentication passwords
14:00-14:50	**Panel:** Internet Wars	**Michael Ligh & Greg Sinclair** Malware RCE: Debuggers and Decryptor Development.	**Mike Renlund** The Big Picture: Digital Cinema Technology & Security.	**Panel:** Black vs. White: The complete life cycle of a real world breach.	**DAVIX Visualization Workshop**
15:00 - 15:50	**Jason Scott** Making a Text Adventure Documentary.	**Igor Muttik** Good Viruses. Evaluating the Risks.	**Taylor Banks & Carric** Pen-Testing is Dead, Long live the Pen Test.		
16:00-16:50		**Chris Eagle & Tim Vidas** Next Generation Collaborative Reversing with IdaPro &CollabReate.	**Tottenkoph, Rev & Philosopher** Hijacking the Outdoor Digital Billboard Network.	**Iclee_vx** Comparison of File Infection on Windows & Linux.	
17:00 - 17:50	**Awards Ceremonies hosted by Dark Tangent**				

Skyboxes

	206	207	208	209	210	211/212
Friday	"Spiders are Fun" party	Hacker pimps		Hardware Hacking Village	Wireless Village	Lockpick Village
Saturday	303	Ninja Networks	i-hacked			
Sunday	HAM Radio Testing	Available	Available			

defcon map



SHOUT OUTS!

The Dark Tangent would like to thank all the people below, and some who shall remain sekret and behind the sceenes:

When you show up to DEF CON and walk through the door you are greeted by the REGISTRATION TEAM (Run by Q and TW who would like to thank: Bart, cstone, Rahael, Reyna, & Tyler, as well as Sharon and the folks from Blaine)

and after you get your BADGE (Thought up by DT, KingPin and Black Beetle, Designed and built by KingPin) Conference CD, the printed program and Lanyard (Neil, Black Beetle, L3d, Nikita)

you might wander past the SCHWAG BOOTH and buy some stuff (Neil, Black Beetle)

and then head down the long all to the CONTEST AREA run by Russr (Who wants to thank DT, Ping, Zac, Charel, Heather, Lock, cotman, Pyr0, roamer, LosTboY, libero, panadero, Phorkus, A, dedhead, R3d, kingpin, stealth, bombnav, ducksauz, voltagespike, sugardaddy, smitty, afterburn, and Parallax.com. Shout outs go to the Security Tribe, KenG, the UAT students, Johnny Long, and my other friends. A special thank you to all the POCs that put their time, effort, money, and brain power into making the contests and other events at Defcon such a resounding success.)

Next to the contest area is the VENDOR AREA, home of cool geek shit, under the watchful eye of Roamer (Who would like to thank Wad, Wiseacre, Evil, and AlxRogan and the DEF CON 16 Vendors.)

Keep your eyes peeled for the GOONS in red shirts. They are constantly helpful & thirsty at the same time, led by Noid (Who thanks his team Adrenaline, Arclight, Captain, Che, Chosen1, CHS, CJ, Converge, Cyber, CyMike, Danozano, Dc0de, flea, Fox Captain, Freshman, GM1, h3adrush, JustaBill, Kevin, Krassi, Londo, Luna, Maximus, Montell, Nobody, P33V3, Pappy, Pescador, David, Priest, Queeg, Quiet, Rik, SkyDog, Spahkle, Vidiot, Xinc, Carric, Kruger, JD)

When the speaking starts it is because SPEAKER CONTROL is running smoothly, led by AgentX (Who thanks #2, Quagmire Joe, Code 24, Amish One, Xam, Crash, Strbik, & Wheatman. AMFYOYO!) and the SPEAKERS have all been managed by Nikita (Who is thanking all the speakers for the many good humored late night chit-chats over impending deadlines and all the priceless awesomeness their content & participation brings to the show. Agent X and his team for herding the cats at the show, Nico for getting all the Feds & MIB to walk a willing line to the podium, Dead Addict, ETA, Black Beetle, Deviant, Cotman, DigitalEbola, Moyer, Kenny and all the rest for being ninja and or pirate..)

While your kicking back in the new CHILL OUT lounge with lighting by Adam Christof, and before the BLACK & WHITE BALL with DJS coordinated by zziks, the WiFi packets will be flowin' thanks to the NOC TEAM. Lockheed is the master of the switch, our very own Netmaster 10baseT, and he is thanking his posse (Many, many thanks to the Network/IT crew that makes this happen every year! We meet up throughout the year at other cons or random travel events to make sure all this happens. Shouts out to Videoman(9 yrs), Heather(8 yrs), effffn (4yrs), Sparky (3yrs), Derek (who couldn't make it this year), Major Malfunction (666 yrs), and our two n00bs this year, Mac and KidKaos!)

When the Goons mobilize, encrypted radios squawking, it's to the beat of DISPATCH which has enjoyed being the voices in your head (Thanks to Benson, Sunshine, Noise, Josy, and Doolittle.)

Almost all the gear that makes the con happens is moved, stored, and watched over by the QM STORE TEAM (Major Malfunction, ETA, Alien, Esteban, Bart, Sqweak and Mags) and they will ninja chop anyone who thinks about messin' with it.

SKY BOX events are managed by Grifter, who would like to thank himself: "Thanks to Grifter for being so fucking awesome, pretty much all of the time! He's an attractive son-of-a-bitch and a real renaissance man when you stop to think about it. And of course I would be remiss if I didn't mention his gorgeous hair; absolutely stunning!"

On site operations are managed by my long time super Ops Master, Zac (Who thanks a lot of people, but I've edited it out because the team leaders have already thanked them!), with Charel coordinating all hotel operations. When Monday finally rolls around and you head home don't forget about all the DEF CON stuff on-line, like the

FORUMS, BLOGS, PICTURE SERVER, and WEB SITE. The network is run by The Dark Tangent, with Forums managed by the ever professional CotMan, Converge, constant web updates by Neil, RogueShadows, and some help from SleeStak. Legal issues handled by Jeff McNamara!

Finally, Shouts to all from The Original Goon, Metalhead... "keep those Juniper Mallets flowing and party safe kids!"