DEFCON
17

Welcome to DEF CON 17!

A couple big changes this year, from a soft opening on Thursday, a new CTF run by DDTEK, expanded DJ and party action by the pool and the chill out area as well as new contests to fill the space of old favorites that couldn't happen this year. The new 1/2 day of newbie and 101 talks should be kicking off, the Cannonball run should be at full speed, the Toxic BBQ is firing up their grills Thursday night, and DJs are getting their sets ready!

I fully expect this year to be smaller than last year by almost 2,000 people, which would be about 25% less due to the economy. This is hard because I still want to do everything we have done in the past, just with less income. So guess what? We are still doing it all! Next year I hope things will recover and will cover the costs of this year.

I didn't want to shrink the con because I figure those who make it here this year deserve something special. If you can make it here then you care about the con, and should be able to go brag to your friends about all the cool stuff they missed out on.

Badges. Well. Remember all that last minute drama from last year with the badges arriving at the last minute? I paid over $15,000 in overnight FedEx fees to get them to the con in time last year, and I wasn't doing _that_ again! So we all got together and planned the badges 6 months early.

We had a working prototype in March. We placed the order for a reduced number due to the economic down turn, and away we went. I swear Murphy lurks on #defcon, because as I write this I don't know what is going to happen with the badges AGAIN! It sux. Chinese customs has decided to hold our box of critical components, of which there are not enough world wide to replace them with in time! I can buy enough extra to make 2,500 badges and then the parts run out unless the box held is released in the next week. Why make them in China you ask? If I were to make the same exact badge in the U.S. it would cost almost 300% more, and there is no way DEF CON can afford that! Note to self: If dealing with customs send many smaller boxes under different manifests so if one gets held up all is not lost.

Many of you have heard about me being appointed to the Homeland Security Advisory Council (HSAC). This is an unpaid position that I donate my time to. I am trying to get more involved where I think I can do the most good as both an outsider and someone who cares about both our infrastructure security and our personal privacy. I never thought such an opportunity would be possible because of how some haters portray DEF CON. Well some people at DHS could see beyond that and I'll try to make the most of it for us all. I hope this signals the beginning of government looking to our generation of security experts to help with fixing all the busted policies and systems we've acquired over the past decades.

Finally, No, I don't qualify as a FED! Nice try. I have no paycheck, no badge, and no arrest authority. But I bet you can spot some around if you look closely - just don't forget we still are running a "spot the undercover reporter" contest as well.

As I like to say, "DEF CON is what you make it" Take the time to introduce yourself and get involved, you won't regret it.

The Dark Tangent

Table of Contents

Policy: Photography and Video Recording

1. No photographing, videotaping, filming, or audio recording without signed consent from the conference attendee being recorded.

2. Photographing, videotaping, or filming crowds is NOT ALLOWED. Exceptions include group photos or other conditions where each person gives explicate permission. Content that does not meet this rule will be confiscated and destroyed.

Capture the Flag (CTF) - binjitsu 2009

All Con until 14:00 Sun

CTF Contest Room

The following teams have demonstrated their uber prowess by qualifying to participate in the DEFCON 17 Capture the Flag Contest: binjitsu, organized by ddtek.

Out of more than 250, 9 teams have been selected to battle last year's champions, sk3wl0fr00t, for the CTF title! DEFCON would like to congratulate all of these talented teams and wish them luck!

VedaGodz

Sexy Pwndas

PLUS

Shellphish

Song of Freedom

lollerskaterz dropping from roflcopters

Routards

WOWHACKER

Sapheads_

alternate teams:

sutegoma

ACMEPharm

Defcon 17 CTF Scoring

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

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

Rather than simply awarding a point per stolen or overwritten key, the scoring system this year will treat keys as commodities (such as diamonds). The following factors are taken into account when deriving a team's overall score:

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

Teams are awarded points as follows:

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

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

Item 5 above is meant to ensure that a team does not simply shut down all of its services in order to achieve a perfect defense.

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

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

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

Toxic BBQ

Thursday at 17:30-21:00 at Sunset Park

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 their time, money and food, and put together a huge kickoff to the con.

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

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

Titanium Chef Challenge

Thursday at the Toxic BBQ

In the tradition of the "Iron Chef" cooking competitions, this contest pits teams against one another in the task of creating a meal focused around a theme ingredient to be revealed right at the start of the contest. More specifics about the rules, along with footage from past years, is available at http://deviating.net/toxicbbq/.

Scavenger Hunt

Friday 12:00-18:00, Saturday 10:00-18:00, Sunday 10:00-12:00

Scavenger Hunt 2k9: We've got the challenge, have you got the skills?

Welcome back to another great year of Finding, Doing, Drinking and Searching. We have compiled an AMAZING List this year that is unlike anything we have ever done in the past. Testing your Hacking, Geeking, Nerding and SEing skills, abilities and knowledge to the absolute limits.

We've taken a big step away from Scavenger Hunts in the past with different challenges based around all aspects of life on-the-hack. Building, DumpsterDiving, Harassing, Seeking, Drinking, Plotting and Planning.

The Rules remain The same:

1. No more than 5 people per team.
2. Siviak is always right.
3. Team with the most points at Noon on Sunday, wins.

With that said, I would like to personally invite back any winners from prior years to compete once again.. The Game has changed, have you kept up?

2nd Annual Podcaster's Meetup

Saturday at 20:00 in Skyboxes 207/208

It's that time of year again, DEFCON, and if you read Justin Foster's blog post, you've altered your Gregorian calendar for it's arrival. Well, this year marks the 2nd Annual Podcasters Meetup at DEFCON! http://pcmeet.squarespace.com/

Here is a quick overview of events for that PCM entails:

What: The Podcaster's Meetup is a LIVE broadcast podcast that includes a panel of all the security podcasters present. Its an event for listeners to meet podcasters and podcasters to meetup with their listeners. Bloggers, coders, hackers, geeks, everyone is welcome to the event, and if you want to be on the show, that just might happen as well.
(Thanks to the I-Hacked.com crew once again!)

Who: So far we have confirmed being there: Security Justice, PaulDotCom, Exotic Liability, Securabit, SMB Minute. (Possibles: Unpersons, GRM n00bs, SploitCast, Phone Losers of America) This is where the hand out of the "I <3 Nikita" boxers will happen, so if you're interested in getting a pair, with all that entails, show up and look for the guys running the event, they'll point you in the right direction, with directions on what to do next.

Sponsors:

- Square Space (coupon code: "defcon" for 10% off the life of their account)
- Astaro

http://pcmeet.squarespace.com/

The Summit

Thursday at 20:45 in the Top of the Riv • Tickets on sale at 20:00 at the DOOR • Ages 16 and older

Join us at the Premier Pre-Defcon Event and hang out with the Geek Gods to support the EFF

The Summit brings together DefCon & Black Hat speakers, past and present, as well as many of the biggest names in the computer security world.

They're coming together in a small, private venue to meet with you! There will be no more the 200 tickets sold, including featured guests. Hosted by Vegas Virtual - Vegas 2.0.
All proceeds from the ticket sales will benefit EFF!
Agenda: Excellent Speakers, Auction, DJ and Dance - mostly in that order

There will also be a separate donating accepted this year for the Make a Wish foundation.

Coffee Wars X

Friday Morning 10:00 - 12:00 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!

"Beverage" Cooling Contraption Contest

Friday at 12:00 - 14:00 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 70° or over 90°, depending on the Las Vegas sun) and cool said beverage to below 40° 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 start your DEFCON off with a blast for free with us!

Hardware Hacking Village

Open Friday-Sunday in Skyboxes 209-210

The Hardware Hacking Village (HHV) this year is a continuation of the tremendously popular event last year. Learn to solder, through hole and surface mount. What's a cap? What's a pot? Learn to build a Parallax propeller chip with our new kit for 2009, but hurry, because quantities are limited. Don't limit yourself to software, come find out where the REAL action is at!

Lockpicking Village

Open Friday-Sunday in Skyboxes 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.

Gringo Warrior

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

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

Hacker Karaoke

Friday at 21:00 in Capri Room 111

Do you like music? Do you like performances? Want to *BE* the performer? Well trot your happy ass to Hacker Karaoke, Defcon's first on-site karaoke experience where you can be a star, even if you don't know it. Don't want to be a star? Well then at hacker karaoke you can also take pride in make an utter fool of yourself. Join Bascule and OverDose in what puts the casbah in "Rock the Casbah"

LosT @ Con Mystery Challenge

All Con [illegible] the Contest Area

The LosT @ Con Mystery Challenge is a yearly hacker contest created by Ryan Clarke (aka "LosT", or "1o57"). So what's it all about? Well it's a mystery.

A few quotes best describe it:

ATDT 421-1057

" LosT spends his free time devising mind-bending puzzles, quandaries and complicated cryptographic conundrums in order push participating hackers to their mental limits. Oddly enough they actually enjoy the intellectual punishment."

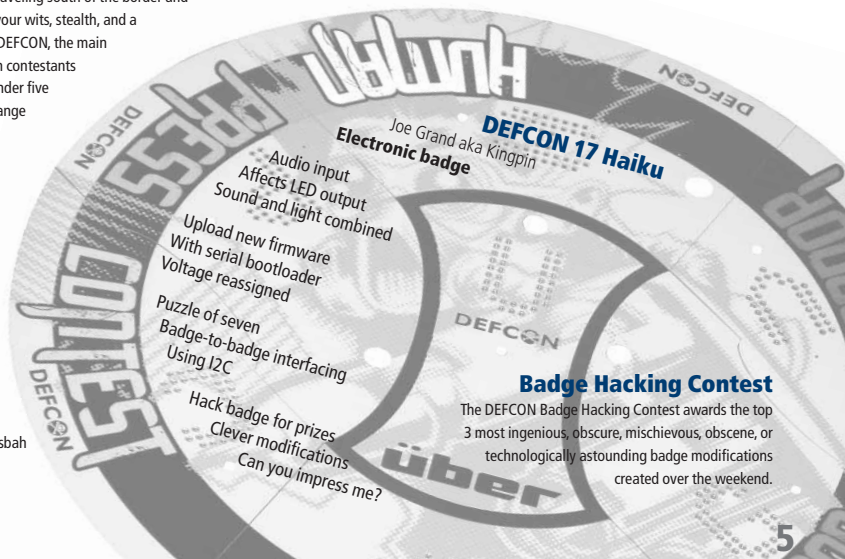
"8 hours later, we opened the locks....with a drill."

"At 1:30 AM (not sure what day this is...no really I don't know) it was only Tim, myself and one stranger that decided to wander in and help. This was 12.5 hours after we received the first box. A small purple box containing clues."

"I'm gonna need some serious reinforcements for next year. ... Props to LosT. That guy owned us good."

+++

If you like a challenge, come play in my world.



EFF FATS

Friday through Sunday in the Contest Area

***Hackers and Guns in Las Vegas— What could possibly go wrong?**

*The Feds hated the idea but the Defcon Goons and attendees loved it. So hell yeah, we're gonna to do it again this year.

Like something out of a Bruce Schneier movie plot contest entry, imagine this scenario. You're a 1337 security expert with mad skills. One night, while kick?n it with your girlfriend, you are both kidnapped by members of a terrorist cell and held in a secret location. These evil doers are attempting to force you to hack infrastructure targets and aid them in advancing their sinister plans. Suddenly SWAT kicks in the door and quickly takes out the bad guys without wasting you or your girl in the process. How do they learn to take out the bad guys without frag'n both your asses? Training, training and more training.

One of the tools they use is a FATS system or Firearms Training Simulator and we got our hands on one for DEFCON 17. But, of course we modded the box to enhance things and added our own special targets. LOL (evil laugh) So?.Step up and test yourself with the real First Person Shooter challenge. No gamer mice, no wimpy Wii wands, just guns, guns and more guns! 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

Team Fortress 2 Tournament

Friday: Open Play, Saturday: Tourney in Royal 2 (Between the Turbo Track and CTF)

TF2 is the best video game made by man. This tournament will pit 6 player teams against one another to determine who the 1337est TF2 team in on the planet (or at least at the Riveria the weekend of DefCon). We will supply the hardware and Audio/Video extravaganza.

You supply the frags.

Hack the Quantum

Capri 114 and 115

Presented by the Joint Qauntum Institute, National Institute of Standards and Technology and University of Maryland, and the Centre for Quantum Technologies, National University of Singapore

With a hands-on Bell-o-meter for entangled photons you can convince yourself that there are quantum effects beyond classical physics: a real qubit is offered to the participant who achieves the strongest violation of a Bell inequality. We also present a fresh attack that breaks many current quantum crypto systems, and demonstrate a photon-based quantum random number generator.

DefCon TV, The Hacker Confessional!

Every year we setup something slightly different for DCTV. We've tried some things so people can upload their own videos that we broadcast over CCTV, but people seldom do (except for music videos of Leonard Nimoy singing the Ballad of Bilbo Baggins). So this year we're sticking it in your face! We have the Hacker Confessional! Backed on the idea of Speaker's Corner, the Hacker Confessional will give attendees the chance to talk for 30 seconds and get up on screen over DefCon TV. Sound may suck, but bonus points for creative methods of communication!

Spot the FED

Almost Same Rules, Different year!

"Like a paranoid version of pin the tail on the donkey, the favorite sport at this gathering of computer hackers and phone phreaks seems to be hunting down real and imagined telephone security and Federal and local law enforcement authorities who the attendees are certain are tracking their every move... Of course, they may be right." - John Markhoff, NYT

Basically the contest goes like this: If you see some shady MIB (Men in Black) earphone penny loafer sunglass wearing Clint Eastwood to live and die in LA type lurking about, point him out. Just get the attention of a red shirt Goon, and they will get Priest to meet with you, and you let him know who you think is a fed. Some feds have already been spotted, so it's best to wait for Priest to show up.

The people around at the time will then (I bet) start to discuss the possibility of whether or not a real fed has been spotted. Once enough people have decided that a fed has been spotted, and the Identified Fed (I.F.) has a say, and informal vote takes place, and if enough people think it's a true fed, or fed wanna-be, or other nefarious style character, you win a "I spotted the fed!" shirt, and the I.F. gets an "I am the fed!" shirt.

Now over the years we have had to modify the rules because there are just too many FEDs out there.

The generally accepted definition is someone sworn with arrest authority.

NOTE TO THE FEDS: This is all in good fun, and if you survive unmolested and undetected, but would still secretly like an "I am the fed!" shirt to wear around the office or when booting in doors, please contact me when no one is looking and I will take your order(s). Just think of all the looks of awe you'll generate at work wearing this shirt while you file away all the paperwork you'll have to produce over this convention.

I won't turn in any feds who contact me, they have to be spotted by others.

DOUBLE SECRET NOTE TO FEDS: This year I am printing up extra "I am the Fed!" shirts, and will be trading them for coffee mugs, shirts or baseball hats from your favorite TLA. If you want to swap bring along some goodies and we can trade. Be stealth about it if you don't want people to spot you. Agents from foreign governments are welcome to trade too, but I gotta work on my mug collection and this is the fastest way.

Ask a red shirt Goon for Major Malfunction, he can sort you guys out with a trade.

Open CTF

Friday at 12:00 until Sunday at 12:00 in the Contest Area

Open Capture The Flag is a hacking contest which any Defcon attendee can play. Contestants connect to the oCTF network and attempt to beat a series of challenges which includes cryptography, malware, developing web exploits, social engineering, forensics and other surprises. All you need to play is something to hack with which can connect via RJ-45 (e.g. laptop). Just remember to use protection when connecting to any foreign network, especially this one.

DENCON Retro Lounge

Royale 2 (Between the Turbo Track and CTF)

Jason Scott of TEXTFILES.COM and Sellam Ismail of VintageTech bring you DENCON, a trip back 30 years in time to some of the earliest days of consumer electronics, home computing, and even the far reaches of what the best engineers might hope to have to themselves. If you're old enough to remember playing with these toys and treasures or young enough to be tired of hearing stories about playing them, this will be your chance all weekend to get hands-on experience, photo opportunities, and even some improvised seminars on these hardware and software dreams.. including a fully working, complete PDP 11/70 system. And we are NOT kidding.

Forum Meet

Thursday at 19:30 in Capri 111

The "Forums Meet" is where we the people/zombies who participate (or lurk) in the Defcon Forums gather to meet each other, finally put a name to a face, catch up on what has been going on since last years Defcon, hangout, mingle, and so on. The Forums Meet is brought to you by Lil_freak, Dallas, meee, and Nikita. (If it wasn't for Nikita we wouldn't have a room to do so this event, so buy her a drink if you see her.)

QueerCon

Friday Prefunk at 16:00 in the Chillout Area, Party at 22:00 in Skyboxes 211/212

Hey all you awesome beautiful queer people--yes, YOU! The Seattle-based Queercon crew is coming back for our sixth year to bring you full-on rainbow awesomeness. Why? Because we love you!

First, come by the chill space for an afternoon prefunk... imagine, a place to meet people where you can actually see them and have meaningful conversations! 4pm-?

Next, dress up and get ready to dance! As always, we'll be throwing the most amazing electronic music dance party EVAR at Defcon.

World of Warcraft Subversion

Friday through Sunday 10:00 to 19:00 in the Contest Area

Information booth on how to use the library we wrote to code character actions in World of Warcraft. And a raffle to win a World of Warcraft account(s).

DEFCON 101

HighWiz, The Dark Tangent, Russr, DJ Jackalope, Deviant Ollam, Thorn, ThePrez98, LosT, Siviak

What is DefCon 101?

With the ever expanding landscape of DefCon: the amount of Games and Contests, the Parties, the Villages, the vast array of Art and Music... All that is going on and to do can be quite daunting to New People beginning their first DefConian adventure. There are even many long time DefCon attendees who come for the talks but may feel overwhelmed or intimidated by many of the other activities happening at the Con. DefCon 101 hopes to change that by providing those people with the information they need to help take the first steps of their journey in the world of DefCon and the DefCon Community.

Unmasking You

Joshua "Jabra" Abraham, Security Expert, Rapid7
Robert "RSnake" Hansen, CEO & Founder, SecTheory

Many people and organizations depend upon proxies and numerous other privacy techniques to mask their true identity. The problem is there are often flaws within these technologies. This talk will demonstrate several of these flaws and as well as weaknesses in well known implementations. There will be several new anti-privacy 0days released.

Wi-Fish Finder: Who Will Bite the Bait

MD Sohail Ahmad, Senior Wireless Security Researcher, AirTight Networks
Prabhash Dhyani, Wireless Security Researcher

Threat of Evil Twin and Honeypots lurking at office parking lots and public hotspots are well known yet awareness level among WiFi users about exposure to such threats remains quite low. Security conscious WiFi users and IT administrators too don't have any simple tools to assess security posture of WiFi clients active in their airspace.

Wi-Fish Finder is a tool for assessing whether WiFi devices active in the air are vulnerable to "phishing" attacks. Assessment is performed through a combination of passive traffic sniffing and active probing techniques. Most WiFi clients keep a memory of networks (SSIDs) they have connected to in the past. Wi-Fish Finder first builds a list of probed networks and then using a set of clever techniques also determines security setting of each probed network. A client is a fishing target if it is actively seeking to connect to an OPEN or a WEP network. Clients only willing to connect to WPA or WPA2 networks are not completely safe either! To find out why , come and attend this talk and witness some live action. There is >50% chance that your laptop will bite the bait!

Tactical Fingerprinting Using Metadata, Hidden Info and Lost Data

Chema Alonso MVP Enterprise Security, CTO Inform·tica64
Jose Palazon "Palako" Yahoo!

In 2003 Tony Blair was "bytten" by a word document which its metadata demonstrated had been edited. Since that days a lot of advisories warning about to keep free of undesired data all published document shown up around the whole Internet... but times went by and people don't worry so much about this BIG problem. In this session you will see how analyzing all published documents in a website is possible to fingerprint a lot of (if not almost all) information about the internal network. This session will show you how to use FOCA tool to collect the files, gathering the information from ODF, MS Office, PDF/EPS/PS files, cross the information found with artificial intelligence rules and fingerprint big amount of info about the network structure, matching IP address with internal server names, printers, shared folders, ACLs...and to show how it can effectively be used by security consultants who traditionally could only offer source code fixes.

Preparing for Cyber War: Strategy and Force Posture in the Information-Centric World

Dmitri Alperovitch, VP Threat Research, McAfee
Marcus Sachs Director, SANS Internet Storm Center
Phyllis Schneck, VP Threat Intelligence, McAfee
Ed Skoudis, Founder & Senior Security Consultant, InGuardians

Cyber warfare is the new hot topic of debate in political and military circles in Washington. This panel of cyber policy experts will explore the definition and reality of a cyber warfare threat, focusing on offensive capabilities and military doctrines of our potential nation-state adversaries, debate the deterrence strategies, and operational and legal frameworks guiding the use of defensive and offensive capabilities of the United States. Finally, the panel will discuss the range of options available to US policy makers for preparing for and responding to a cyber attack on this country.

Down the Rabbit Hole: Uncovering a Criminal Server

Iftach Ian Amit Director, Security Research, Aladdin

In this talk I'll cover the research efforts done when we managed to come across a criminally operated server running the latest Neosploit (and other goodies).

During the research there have been several crucial points of interest such as the discovery of compromised credentials, getting into the applications used by the criminals to manage the infections, and the infection channels, as well as a few hairy moments of being logged in to the server while "someone" else was also logged in (from a notorious location that has been brought down after an article at the Washington Post - McColo...).

Pre-Con Introduction to Lock Picking

Alek Amrani Longhorn, Lock Picking Club Officer

Make it out before DEF CON starts, and venture into lock sporting with the Longhorn Lock Picking Club. Learn to lock pick from one of the largest lock sporting organizations in the western hemisphere. This is a great opportunity for anyone trying to dodge the incredibly popular (read: crowded) Lock Picking Village but don't want to try learning on their own.

Session Donation

Alek Amrani

It's easier to give away than it is to take. Apply that theory to Session Hijacking, and enter Session Donation.

Session Donation is a computer session attack that attempts to gain information by taking session hijacking in an entirely new direction. Session Donation is an interesting new spin on an old attack that is much harder to prevent than it's predecessor, and equally as dangerous.

Your Mind: Legal Status, Rights and Securing Yourself

James "Myrcurial" Arlen Security Researcher
Tiffany Rad, President, ELCnetworks and Adjunct Professor at University of Southern Maine's Computer Science Department

As a participant in the information economy, you no longer exclusively own material originating from your organic brain; you leave a digital trail with your portable device's transmitted communications and when your image is captured by surveillance cameras. Likewise, if you Tweet or blog, you have outsourced a large portion of your memory and some of your active cognition to inorganic systems. U.S. and International laws relating to protection of intellectual property and criminal search and seizure procedures puts into question protections of these ephemeral communications and memoranda stored on your personal computing devices, in cloud computing networks, on off-shore "subpoena proof" server/jurisdiction-hopping platforms, or on social networking sites. Although once considered to be futuristic technologies, as we move our ideas and memories onto external devices or are subjected to public surveillance with technology (Future Attribute Screening Technology) that assesses pre-crime thoughts by remotely measuring biometric data such as heart rate, body temperature, pheromone responses, and respiration, where do our personal privacy rights to our thoughts end and, instead, become public expressions with lesser legal protections? Similarly, at what state does data in-transit or stored in implantable medical devices continuously connected to the Internet become searchable? In a society in which there is little differentiation remaining between self/computer, thoughts/stored memoranda, and international boundaries, a technology lawyer/computer science professor and a security professional will recommend propositions to protect your data and yourself.

CSRF: Yeah, It Still Works

Mike "mckt" Bailey ASS
Russ McRee, ASS

Bad News: CSRF is nasty, it's everywhere, and you can't stop it on the client side.

Good News: It can do neat things.

CSRF is likely amongst the lamest security bugs available, as far as "cool" bugs go.

In essence, the attack forces another user's browser to do something on your behalf.

If that user is an authenticated user or an administrator on a website, the attack can be used to escalate privilege.

We've identified an endless stream of applications, platforms, critical infrastructure devices, and even wormable hybrid attacks, many of which require little or no Javascript (XSS).

The key takeaway is this: a vulnerability that is so easily prevented can lead to absolute mayhem, particularly when bundled with other attacks. Worse still, identifying the attacker is even more difficult as the attack occurs in the context of the authenticated user.

The presentation will discuss a variety of attack scenarios, as well as suggested mitigation.

Sniff Keystrokes With Lasers/Voltmeters: Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage

Andrea Barisani, Chief Security Engineer, Inverse Path Founder & Project Coordinator, oCERT
Daniele Bianco, Hardware Hacker, Inverse Path

TEMPEST attacks, exploiting Electro Magnetic emissions in order to gather data, are often mentioned by the security community, movies and wanna-be spies (or NSA employees we guess...).

While some expensive attacks, especially the ones against CRT/LCD monitors, have been fully researched and described, some others remain relatively unknown and haven't been fully (publicly) researched.

Following the overwhelming success of the SatNav Traffic Channel hijacking talk continue with the tradition of presenting cool and cheap hardware hacking projects.

We will exploring two unconventional approaches for remotely sniffing keystrokes on laptops and desktop computers. The only thing you need for successful attacks are either the electrical grid or a distant line of sight...and no expensive piece of equipment is required.

We will show in detail the two attacks and all the necessary instructions for setting up the equipment. As usual cool gear and videos are going to be featured in order to maximize the presentation.

The Middler 2.0: It's Not Just for Web Apps Anymore

Jay Beale, Co-Founder, InGuardians
Justin Searle, Sr. Security Analyst, InGuardians

The Middler is a next-generation man-in-the-middle tool that takes the focus beyond the raw mechanics of the protocol on to the application itself. New for Def Con, it now can man in the middle Voice over IP (VoIP), producing the opportunity to interactively redirect calls, join them, or take them over. All of these effects join The Middler's goal of putting the victim into a kind of matrix by implementing man in the middle attacks specific to each web application. We've also added a graphical interface, allowing for interactive target selection based on information that The Middler gathers about potential victims. We've added more applications and enhanced the set of non-application specific capabilities, including easy session cloning, IFRAME injection and a Java script exploit library that can force the user into the Browser Exploitation Framework (BeEF) or a Metasploit exploit. This demo-filled talk will enhance your man in the middle powers just in time for one of the most hostile networks ever seen.

A Low Cost Spying Quadrotor for Global security Applications Using Hacked Commercial Digital Camera

Antoine Gademer & Corentin Chéron

Accessing centimetric georeferenced images is crucial for local military or civil intelligence, reconnaissance and surveillance applications. When classical satellite or aerial imagery is not available the Unmanned Aircraft Systems (UAS) are often a very interesting solution. But having an operational UAS for spying operations implies to solve the following practical problems:

- Design and realize a reliable flying micro-UAS develop efficient tools for real-time navigation to ensure that the UAS will cover all target points merging all trajectory data for real-time georeferencing of high resolution imagery
- Design appropriate software for optimal data exploitation

We present our practical solutions to these different points.

The last technological lock with on-the-shelf retail cameras is the ability to control them in real-time with limited computational resources. To achieve the reactivity and flexibility needed for professional imagery we need to do some reverse engineering on our camera to take full control on the power on/off, on the trigger and most importantly on the dating of the pictures. We will present the reasoning and the result we obtain in our case.

At last we will present how, with the trajectory and the precise dating of the picture, we are able to construct very quickly the georeferenced footprint database of the pictures and thus allow the user to navigate in the data few minutes after the data retrieving. The whole visualization and navigation is made in Google Earth by using smart usage of the KML format.

Beckstrom's Law: A Model for Valuing Networks & Security

Rod Beckstrom

Beckstrom's Law is a new model or theorem of economics formulated by Rod Beckstrom. It purports to answer 'the decades old question of "how valuable is a network." It is granular and transactions based and can be used to value any network. It applies to any network: social networks, electronic networks, support groups and even the Internet as a whole. To read a white paper explaining the law and mathematics in detail, please see Economics of Networks. This new model values the network by looking from the edge of the network at all of the transactions conducted and the value added to each. It states that one way to contemplate the value the network adds to each transaction is to imagine the network being shut off and what the additional transactions costs or loss would be.

Beckstrom's Law differs from Metcalfe's law, Reed's law and other concepts that proposed that the value of a network was based purely on the size of the network, and in Metcalfe's law, one other variable.

Robot Shark Laser! What Hackerspaces Do

Beth FreeSide, dc404 & KaosTheory Security Research
Noid BlackLodge
Nick Farr, HacDC
Leigh Honeywell, HackLab
Steve Clement, Syn2cat

Ever wonder what they mean by 'Fight Club for Nerds'? Do you daydream about what you could do if you had an underground lab and minions or a workshop and helpers? Have you considered all the ways to incorporate lasers into your life? Are you sure about that? Come see what the evil geniuses at HackerSpaces far and wide have built and how.

This panel of diverse hackerspace members, will show you step by step how they built their favorite projects, including video and live demos, and Q & A.

Hijacking Web 2.0 Sites with SSLstrip

Sam Bowne Instructor, City College San Francisco, Computer Networking and Information Technology Department

Many Websites mix secure and insecure content on the same page, like Facebook. This makes it possible to steal all the data entered on such a page easily, using Moxie Marlinspike's new SSLstrip tool. First I will give a brief explanation and demonstration of the technique, and then I will help audience members set up the attack themselves on their own laptops. Detailed instructions and all required software will be provided. Audience members should bring a laptop computer to participate in the hands-on training.

Design and Implementation of a Quantum True Random Number Generator

Sean Boyce, Security Researcher

The problem of generating "reasonable" approximations to random numbers has been solved quite some time ago… but this talk is not for reasonable people. Generating true random numbers with a deterministic system is impossible; and so we must drink deeply from the raw, godless chaos of quantum physics.

This talk will cover the various pitfalls of quantum true random number generator construction, including bias, statistical relatedness between bits, and unpleasant supply voltages. A working reference design that overcomes these hurdles will be described, and barring major disaster, demonstrated. Notably, this design contains a custom, fully solid-state particle detector that may be constructed for around USD $20.

BitTorrent Hacks

Michael Brooks & David Aslanian

This is the journey of two pirates hacking BitTorrent. This talk will cover ways of abusing the BitTorrent protocol, finding vulnerabilities in BitTorrent clients and exploiting them. We will also cover counter measures to these attacks.

Old Skool Brought Back: A 1964 Modem Demo

K.C. Budd "Phreakmonkey", Security Researcher
Taylor Banks "Dr Kaos", Security Researcher

Eighteen years ago I was given a curious device: An Acoustic Coupled modem in a wooden box. I've kept it over the years and recently rediscovered it. Thanks to the recent invention of the web, I am now able to discover something about its history; I may have the oldest working modem on the planet! At this talk I will not only show you the modem, but also demonstrate its operation. Come along for a journey 45 years back to the beginning of digital telecommunications!

Hadoop: Apache's Open Source Implementation of Google's MapReduce Framework

Joey Calca Hacked Existence Team
Ryan Anguiano Hacked Existence Team

This presentation will begin with a brief overview of Google's Map/Reduce Framework. Map/Reduce is built to analyze extremely large datasets. We will first look at what a Mapper and Reducer are, the inputs they take and the outputs they generate. From there, we will look at the open source java based implementation of the Map/Reduce Framework by the Apache Team's Hadoop Project. Since Hadoop is Java based, we will then look at using the Hadoop framework in order to build Mappers and Reducers in Python, as well as running Mappers written in the AWK scripting language. A brief comparison of compile times and efficiencies between the three will be shown, as well as the results from running our code on ASU's Saguaro Cluster. After that, we will brush over HBase, the Hadoop equivalent to Google's BigTable, a non-relational database for Map/Reduce. Finally, we will look at some demo code, including a machine learning algorithm based on the Netflix Prize Dataset, a 2 gigabyte dataset of movie ratings from the Netflix Database.

Also, we will not present on, but will include source code from different team's projects, including Map/Reduce programs for image analysis and recognition, analyzing air traffic data, analyzing package delivery systems for use with swarm theory and a Map/Reduce program that analyzes patterns in large literature as a response to "The Bible Code", most of which use public datasets as inputs.

Computer and Internet Security Law: A Year in Review

Robert Clark, Attorney

This presentation reviews the important prosecutions, precedents and legal opinions of the last year that affect internet and computer security. We will discuss the differences between legal decisions from criminal cases and civil lawsuits and what that means to the security professional. This presentation is strongly audience driven and it quickly becomes an open forum for questions and debate. This year the past key precedents have involved: the Fifth Amendment and passphrases to an encrypted hard drive (UPDATE- the case is in and Government wins appeal. The Defendant MUST produce an unencrypted hard drive to the grand jury!!!); Fourth Amendment searches; Pirate Bay prosecution in Sweden; use of CFAA in civil cases against departing employees and trade secrets; forensics and use of metadata; FTC injunction against CyberSpy software and its RemoteSpy; reverse engineering; Facebook and privacy rights; and, a case of forensics to support a default judgment

Black / _White_

We get it. DEFCON is a techno-fetishists wet-dream -- but it is possible to overdose (watching all of that binary, hex, octal, IPv4 and IPv6 fly by all day can drive one to insanity). That's why the DCCTPPPHS (DEFCON Committee for Mind Contr-er-Cognitive Therapy and Physiological Pampering for the Progression of the Hive State) enforces a strict partying policy. All "individuals" may (will) check in with some (all) of the three types of events that go on during Friday and Saturday:

During the daytime, from 10am to 6pm - come join us in Capri Rooms 101 & 102 for the Wireless "ChillOut" Lounge, for a relaxing session on the conference wireless. Release all that pent up tension and free up those ports-er-that bad Qi that's been building up - as our talented and diverse set of DJs serenade your carpal-tunnel-ridden fingers on a journey to mystical places (like the holy wall of Ovis Aries).

If that's not enough for your slowly conforming mental state, the madness picks up where the ChillOut Lounge leaves off at the Riviera pool from 6pm til 11pm! Get your dose of fresh non-artificially-oxygenated air, grabs some drinks, enjoy the "cultured" and historical Riviera scenery, and watch the sky plunge into the dark void overhead as the DJs continue to rock your body and mind.

But that's not all DCCTPPPHS has in store for your weak soul...

Just when you think your body can't take anymore of the copious and absurd amounts of fun we've injected into your stream of consciousness (and the Riv purveyors have more than likely injected into your bloodstream), be prepared to submit to the ultimate in aural and visual enlightenment with: The Black & White Balls, which go from 8pm to 3am (also held in Capri Rooms 101 & 102)! Both feature world renowned talent and con favorites! Costume-attire strongly suggested!

On Friday night, fall into the darkness at the Black Ball as the musical talent sways you with their nefarious hedonistic party rock, industrial, breaks, electro, drum'n'bass, and psytrance. After giving in to your darkest pleasures, the White Ball on Saturday will wash off the grimethat's saturated every living inch of your body–accomplished by the ancient art of "booty-shake" - a talent that our crack-squad of DJs have refined through years of rigorous training in picking out the creme de la creme of banging glitch-hop, breaks, drum'n'bass, progressive and house music tracks.

You will attend.

You will conform.

In the words of the DCCTPPPHS Grand Enlightened Overseer and Arbiter

Scott: "Resistance is pretty much futile."

Chillout

Chillout Day 1: Friday, July 31, 10:00-18:00

Fillmatic
ClimaxSD.com - http://myspace.com/theimperialwizardfillmatic

DJ Rene
(Icarus Productions, Beauty and Da beat, Hiball)
http://djrene.org

DJ njnTrubl
(Dead Monk Society, Submersible DJs, Neighborhood Productions, Pendulum Productions)
http://www.myspace.com/njntrubl

8thNerve
http://soundcloud.com/dj8thnerve

Pepse
(Swell Records, Desert Trance Society, StayChooned)
http://DanceMusicBlog.com

DJ Felix Kay
http://soundcloud.com/dj-felix-kay

Digital Phreak - (Digital Autopsy)
http://myspace.com/ifnmadeit

Corruptdata
http://myspace.com/CorruptData

Chillout Day 2 (NSBRadio.co.uk Live Broadcast): Saturday, August 1, 10:00-18:00

Undecided (System Recordings, Mob Records,Sango-Music, Muti Music)
http://www.undecidedonline.com/

TRONA - (System Recordings, Seattle)
http://tronamusic.com and http://myspace.com/trona

DJ Reeves - (KC Raver, Chillfactor Productions, Dominion Group Entertainment, NSBradio.co.uk)
www.myspace.com/dj_reeves

HoaX - (Nubreaks.com, SoundcheckRadio.co.uk)
http://myspace.com/Hoax408

Inconspicuous Villain - (NSBradio.co.uk)
www.myspace.com/villainism

Simo Sleevin - (Sleevin.com, NSBRadio.co.uk)
http://sleevin.com

Simon Plexus - (NSBRadio.co.uk)

The Scritch - (NSBRadio.co.uk, Raindance Presents, Dax Presents)

Pool Party!

_POOL PARTY! (NSBRadio.co.uk Live Broadcast): Friday, July 31, 18:00-23:00

The Scritch - (NSBRadio.co.uk, Raindance Presents, Dax Presents)

Inconspicuous Villain - (NSBradio.co.uk)
www.myspace.com/villainism

_POOL PARTY!
Saturday, August 1, 18:00-23:00

DJ Reeves - (KC Raver, Chillfactor Productions, Dominion Group Entertainment, NSBradio.co.uk)
http://myspace.com/dj_reeves

HoaX - (Nubreaks.com, SoundcheckRadio.co.uk)
http://myspace.com/Hoax408

Simo Sleevin - (Sleevin.com, NSBRadio.co.uk)
http://sleevin.com

DJ AMP
http://myspace.com/vegasbreaks

Simon Plexus - (NSBRadio.co.uk)
http://iwtf.net

Pepse - (Swell Records, Desert Trance Society, StayChooned)
http://DanceMusicBlog.com

DJ Felix Kay
http://soundcloud.com/dj-felix-kay/

8thNerve
http://soundcloud.com/dj8thnerve

Black Ball

Friday, July 31, 20:00-03:00

RECOGNIZE: The Goon Band - (DEFCON, 303, SecurityTribe, The Shmoo Group)
http://defcon.org / http://securitytribe.com / http://shmoo.org

Saturday, August 1, 20:00-03:00

Phylo - (NSBRadio.co.uk) http://phylomusic.com

E-Roc - (DNBRadio.com, NSBRadio.co.uk) http://myspace.com/dieroc

VJ Q.Alba
http://soundcloud.com/sigtrap

Mitch Mitchem http://IHaveAGiantDick.com

SailorGloom - (DEFCON. Agents of Empire DJs. Our-Darkness, Stuttgart. Dungeon, Waikiki. Therapy, San Diego) http://www.myspace.com/sailorgloom

Great Scott
(Muti Music, Glitch.FM, NSBRadio.co.uk, KTRU) http://djgreatscott.com

Krisz Klink - (DEFCON, Kontrol Faktory, Zombie Zoo, Batcave LA)
http://myspace.com/kriszklinka

Undecided
(System Recordings, Mob Records, Sango-Music, Muti Music) http://www.undecidedonline.com/

njnTrubl - (Dead Monk Society, Submersible DJs, Neighborhood Productions, Pendulum Productions) -
http://www.myspace.com/njntrubl

Miss DJ Jackalope (DEFCON) - http://dj-jackalope.com

TRONA - (System Recordings, Seattle) http://tronamusic.com - http://myspace.com/trona

Mumpi - (Phonoelit DJ Crew) www.phonoelit.org

Snow Crash http://soundcloud.com/snow-crash/ • http://last.fm/music/snow+crash

White Ball

(no actual trial) against a party that used several file deletion programs to hide and delete evidence.

De Gustibus, or Hacking your Tastebuds

Sandy Clark "Mouse", University of Pennsylvania

Do you geek out over food? Do you rave over a particular vintage? Do you get into fights about relative merits of belgain vs. swiss chocolatiers? Know the difference between a Gourmet and a Gourmand? Ever done a real chocolate tasting? Wondered what's the big deal with food/wine parings? Ever tried Miracle Fruit? Like any other electrical/chemical machine the body can be hacked and that includes the tastebuds. Let's discuss taste, and then let's taste stuff! For a small fee (< $2) you can choose to take part in a food/wine paring, A blind chocolate tasting (rating forms, will be provided, see how you compare to the experts) or experiment with Miracle Fruit (along with many things to try it out on), Real Vintage Balsamic Vinegar (like syrup) - Also feel free to bring something you've discovered and want others to try.

Confidence Game Theater

Cough, Security Researcher

This presentation will include a brief discussion of the history, nature, and basic principles behind Confidence Games. The bulk of the presentation we will be acting out some Confidence Games in skit form.

Lockpicking Forensics

Datagram

Lockpicking is portrayed as the ultimate entry method. Undetectable and instantaneous as far as films are concerned. Nothing is further from the truth, but freely available information on the topic is nearly impossible to find. This talk will focus on the small but powerful fragments of evidence left by various forms of bypass, lockpicking, and impressioning. Attendees will learn how to distinguish tool marks from normal wear and tear, identify the specific techniques and tools used, and understand the process of forensic locksmithing in detail.

Death of Anonymous Travel

Sherri Davidoff Philosecurity

Worldwide, people who use cars, buses, trains, and carry cell phones are tracked in increasingly centralized corporate and government databases. This capability is still in its infancy, and has been facilitated by payment systems which are linked to identification and refer to centralized electronic databases.

Mass tracking and surveillance capabilities have arisen organically, often as side effects of new technologies, and are being increasingly leveraged by government and law enforcement in the name of national security. For security purposes, the public is generally not provided with detailed information about the management and use of mass surveillance systems.

As a result, relatively small groups are able to track and control the movements of average citizens around the world, every minute of every day. These systems are opaque, not well documented, publicized or regulated.

The purpose of this presentation is to:

- Collate and disseminate information about current known travel monitoring practices;
- Discuss technical and social solutions for maintaining personal privacy and the freedom to assemble;
- Encourage greater transparency and public control over data collection and use.

The presentation will include a Touch-and-Feel Fare Collection table, where attendees can browse the speaker's historical collection of automobile, coach, subway, telephone, and airline fares/tokens/passes. Attendees are welcome to non-destructively analyze electronic devices with magstripe/RFID readers and other tools.

Unfair Use–Speculations on the Future of Piracy

Dead Addict

Piracy has always been a sophisticated, if not chaotically organized effort—from acquisition, packaging, distribution, risk analysis and managing criminal volunteers.

Piracy has moved from software, to all mediums—books, comic books, knitting patterns, video medium of all kinds. Despite distinctions in types of piracy, there are evolutionary measures that need to take place to address a number of challenges. Between malware codecs, root-kitted software, attempts to flood distribution networks with bad information, and other attacks, there are problems to be solved.

The future will involve distributed architectures, data integrity measures, reputation management via digital signatures, and standardization of metadata.

I will discuss the state of piracy, and touch as need on its past, then discussing future technologies to address current and upcoming challenges.

This talk will not spend time discussing the law or ethics, although the distinction between piracy and bootlegging will be made.

Eye patches optional.

DEFCON 1: A Personal Account

Dead Addict

As time slips away, so do the memories of cons past.

In this talk I'm going to talk about DC1, its planning, execution, components, and challenges.

I'll give snippets of seemingly practical advise; don't design T-shirts with lots of dense text on the back, no matter how clever. I'll discuss of obvious misjudgments; don't invite both the prosecutor and the subject of an active prosecution without warning the parties. I'll also have some minor show and tell: first badge, first T-shirt copies of DC1 tapes, sketch of original DC1 logo.

With luck some old DC1 speakers will show up as well.

AAPL: Automated Analog Telephone Logging

Da Beave, Security Researcher &
JFalcon, Security Researcher

Since 1983 when Hollywood introduced "Wardialing" to the public, there has been little change in the methods involved. While some pieces of hardware attempted to take it beyond what was essentially a telephonic "ping" scan, the methods and technology didn't maintain that momentum. However, thanks to modern computing and open source software tools, we are now able to cartograph an entire phone exchange in one pass while discerning voice, tones, faxes and modems. With some creative processing, it might be taken even farther into speech recognition

Who Invented the Proximity Card?

Michael L. Davis

Who invented the first Proximity Card System? And what security company dismissed it as a mere magician's trick? And what does this have to do with goldfish? Stop by and take a trip down memory lane as we explore the history of a prolific inventor who was one of the founding fathers of the physical security industry. (Hint: This person was a musician with perfect pitch whose first patent was for an automatic garage door opener.)

Con Kung-Fu: Defending Yourself @ DEFCON

Rob "Padre" DeGulielmo

After the authors laptop fell victim to a slick redirection technique and subsequent malicious .lzm injection and MBR Trojan infiltration during DEFCON 16 he thought it would be interesting to talk about the episode (besides, his psychotherapist recommended it), and give new con-goers some tips and tricks to help them avoid the same fate. We will see a demonstration of a typical wireless subversion, and will learn how to avoid it. This talk should give attendees some interesting tools to play with while they are at con, while allowing their laptops to go unhacked for 5 minutes.

Packing and the Friendly Skies (Why Transporting your Firearms may be the best way to Safeguard your Tech when you Fly)

Deviant Ollam, Unicorn Phrenologist

Many of us attend cons and other events which involve the transportation of computers, photography equipment, or other expensive tech in our bags. If our destination if far-flung, often air travel is involved… this almost always means being separated from our luggage for extended periods of time and entrusting its care to a litany of individuals with questionable ethics and training.

After a particularly horrible episode of baggage pilferage and equipment theft, I made the decision to never again fly with an unlocked bag. However, all "TSA compliant" locks tend to be rather awful and provide little to no real security. It was for this reason that I now choose to fly with firearms at all times. Federal law allows me (in fact, it REQUIRES me) to lock my luggage with proper padlocks and does not permit any airport staffer to open my bags once they have left my possession.

In this talk, I will summarize the relevant laws and policies concerning travel with firearms. It's easier than you think, often adds little to no extra time to your schedule (indeed, it can EXPEDITE the check-in process sometimes), and is in my opinion the best way to prevent tampering and theft of bags during air travel.

Sharepoint 2007 Knowledge Network Exposed

Digividual

Microsoft released a free add on to Microsoft Sharepoint Server 2007 called the Knowledge Network. At the time it seemed like an entry in the Total Information Awareness initiative, though it was never called that in any official form. This talk will dissect the features offered by the Knowledge Network and offer speculations as to what Microsoft might have running already.

Socially Owned in the Cloud

Digividual

This talk will present a survey of the most popular cloud/web applications and their responses to a questioner regarding their data retention, data ownership, their commercial use of the data they have harvested. Furthermore it will explore their data retention following a death. What happens if a provider company goes bankrupt?

Why Tor is Slow, and What We're Doing About It

Roger Dingledine

Many of you have probably tried Tor, and then stopped because you found it too slow. Now that Tor has several hundred thousand users, our original design decisions are showing their age. We need to figure out and deploy some major changes if we want the Tor network to scale up to the million-user mark.

Problem #1 is that Tor's congestion control does not work well. We need to come up with ways to let "quiet" streams like web browsing co-exist better with "loud" streams like bulk transfer. Problem #2 is that some Tor users simply put too much traffic onto the network relative to the amount they contribute, so we need to work on ways to limit the effects of those users and/or provide priority to the other users. Problem #3 is that the Tor network simply doesn't have enough capacity to handle all the users that want privacy on the Internet. We need to develop strategies for increasing the overall community of relays, and consider introducing incentives to make the network more self-sustaining.

In this talk I'll walk through these problems and more: why we think these are the right problems to solve, and how we're solving them.

Attacking SMS. It's No Longer Your BFF

Brandon Dixon, Information Systems Security Engineer, G2

It's the year 2009 and spam mail is still taking up a huge percentage of all email sent everyday over the Internet. Could you imagine that same messaging spam making a detour through your favorite cellular provider gateway and right to your SMS inbox? Mobile spam has not reached the same popularity as email spam, but what if it was as easy as submitting a form to spam thousands of people?

Personal Survival Preparedness

Steve Dunker, Associate Professor, Northeastern State University
Kristie Dunker, The Swag Assistant

When the sewage hits the oscillating blades of death, will you be ready? A Las Vegas Survival Scenario will be presented to the audience at the start of the lecture. This talk will concentrate on disaster preparedness at the individual and/or family level. General overall preparedness will be covered as well as specific disasters such as terrorism, epidemic, nuclear, technical, and natural catastrophes. At the end of lecture the scenario answer will be given. Be ready to test yourself against your Defcon brethren and the denizens of Las Vegas—will you survive the high mortality rate?

Advanced MySQL Exploitation

Muhaimin Dzulfakar, Security Consultant, security-assessment.com

This talk focuses on how MySQL SQL injection vulnerabilities can be used to gain remote code execution on the LAMP and WAMP environments. Attackers performing SQL injection on a MySQL platform must deal with several limitations and constraints. For example, the lack of multiple statements in one query makes MySQL an unpopular platform for remote code execution compared to other platforms. This talk will show that arbitrary code execution is possible on the MySQL platform and explain the techniques. In this presentation, the author will release a new tool titled MySqloit. This tool can be integrated with metasploit and is able to upload and execute shellcodes using a SQL Injection vulnerability in LAMP or WAMP environments.

30k Feet Look at WiFi

Luiz "efffln" Eduardo

Although inflight wee-fee service is really nothing new... (some airlines have had it for a while, some even already gave-up on the service), in the past year it's got some traction again with the release of the service by some airlines in the US and some other countries. The talk will cover things like wi-fi infrastructure, auth stuff, spectrum analysis, protection mechanisms (if any), general usage, user device types and uplink technology that actually makes the user hit the "tubes". Data collected a few years ago in flights using older technologies, as well as data collected in newer ones and the possible use of tools available will be discussed.

Using Guided Missiles in Drive-Bys: Automatic Browser Fingerprinting and Exploitation with Metasploit

Egypt, Core Developer, Metasploit Project

The blackhat community has been using client-side exploits for several years now. Multiple commercial suites exist for turning webservers into malware distribution centers. Unfortunately for the pentester, acquiring these tools requires sending money to countries with no extradition treaties, taking deployed packs from compromised webservers, or other acts of questionable legality. To ease this burden the Metasploit Project will present an extensible browser exploitation platform integrated into the metasploit framework.

Hello, My Name is /hostname/

Endgrain, Student of Computer Science, University of Southern Maine
Tiffany Rad, Part-time Professor, Computer Science Department, University of Southern Maine
Dan Kaminsky, Director of Pen Testing, IOActive

It is widely known that MAC addresses are spoofable, however many access control models rely on them to uniquely identify devices. When host names are set to be user's real names and are broadcast to the Internet and accessible with reverse DNS lookups, everybody on the Internet, with no work, knows exactly who you are. You can't do medical research without saying JANE PHILLIPS IS CURIOUS ABOUT PREGNANCY and you can't study the effects of marijuana without TOM STEVENS IS READING UP ON SMOKING OUT. We will discuss the technical, legal, and ethical implications of transparency of identity online versus the war on combating piracy and how it pressures IT departments to design and maintain systems with these fallacies.

Runtime Kernel Patching on Mac OS X

Bosse Eriksson, Security Researcher, Bitsec

Runtime kernel patching has been around for almost ten years and is a technique frequently used by various rootkits to subvert the kernel's used in many modern operating systems.

This technique does not require any types of kernel modules or extensions and will allow you to hide various things like processes, files, folders and network connections by modifying the kernel's memory directly. It will also allow you to place various backdoors in the kernel for privilege escalation.

This talk will discuss runtime kernel patching on Apple's operating system Mac OS X and the XNU kernel. We will cover some rootkit basics as well as some Mac OS X specific 'features' which will facilitate our journey into the deepest parts of the darwin operating system and the XNU kernel.

As a bonus we will also show some basic methods for rootkit detection on Mac OS X that will aid you in the process of detecting rootkits that utilize runtime kernel patching to stay hidden.

Hacking the Apple TV and Where your Forensic Data Lives

Kevin Estis, Security Researcher
Randy Robbins, Security Researcher

This is a primer for both newbie Apple TV hackers and digital forensics investigators. The intent of the presentation is to show how easy it is to modify an Apple TV to run 3rd-party applications and also point out where the Apple TV tracks your activities (including files played, applications installed, and connected networks).

Social Zombies: Your Friends Want to Eat Your Brains

Tom Eston, Social Media Security Researcher
Kevin Johnson, Senior Security Analyst, InGuardians

Tom Eston and Kevin Johnson explore the various concerns related to malware delivery through social network sites. Ignoring the FUD and confusion being sowed today, this presentation will examine the risks and then present tools that can be used to exploit these issues.

This presentation begins by discussing how social networks work and the various privacy and security concerns that are caused by the trust mass that is social networks. We use this privacy confusion to exploit members and their companies during our penetration tests.

The presentation then discusses typical botnets and bot programs. Both the delivery of this malware through social networks and the use of these social networks as command and control channels will be examined.

Tom and Kevin next explore the use of browser-based bots and their delivery through custom social network applications and content. This research expands upon previous work by researchers such as Wade Alcorn and GNUCitizen and takes it into new C&C directions.

Finally, the information available through the social network APIs is explored using the bot delivery applications. This allows for complete coverage of the targets and their information.

dradis Framework: Sharing Information Will Get You Root

etd, Senior Security Consultant, NGS Software

dradis is not a dream any more. It is a mature framework. Information sharing taken to a new level. If you are in the security industry is because you want to break stuff. Not because you like wasting your time. Not because you love to write reports. Not because you enjoy doing things twice, or doing them manually if they could be scripted up. dradis' aim is to let you focus on what you like by making all the overhead something not to worry about.

Cracking the Poor and the Rich: Discovering the Relationship Between Physical and Network Security

Damian Finol

Is there a relationship between physical and network security? this presentation tries to uncover some information about the possible relationship between physical and network security by looking at how the rich and the poor in Venezuela implement both physical tools (like electric fences, bulletproof windows, etc) and network wireless encryption techniques (WPA2, WPA, WEP, none). By using simple tools like Kismet, a laptop, and a really fast car the speaker sniffs the wireless networks of both the dangerous slums and the rich areas and uncovers an interesting relationship between them both.

Attacking Tor at the Application Layer

Gregory Fleischer, Security Researcher

Surfing the web using Tor makes you invincible, right?

Wrong! Between the technical deficiencies, web browser idiosyncrasies, Tor vulnerabilities, social engineering, and bone-headed user decisions, there is ample room for attack and exploitation.

This presentation covers past and present application layer attacks against Tor. From practical hacking and ControlPort madness, to the most up-to-date techniques and beyond, this is an in-depth, technical look at active client-side attacks, HTML content injection, browser fingerprinting, network leakage and other relevant anonymity set issues.

So, forget about the over-heated nodes, infinite circuits and magic packets. When anyone with some JavaScript knowledge, a server on the Internet and a little bit of cleverness can launch these attacks, now is the time to start paying attention to how you use Tor.

Hacking the Smart Grid

Tony Flick

The city of Miami and several commercial partners plan to rollout a "smart grid" citywide electrical infrastructure by the year 2011. This rollout proceeds on the heels of news that foreign agents have infiltrated our existing electrical infrastructure and that recent penetration tests have uncovered numerous vulnerabilities in the proposed technologies. Simultaneously, the National Institute for Standards in Technology (NIST) has recently released a roadmap for producing Smart Grid standards. In this Turbo Talk, I will discuss the flaws with the current guidelines and map them to the criticisms of similar regulatory mandates, including the Payment Card Industry Data Security Standard (PCI DSS), that rely heavily on organizations policing themselves.

Router Exploitation

FX of Phenoelit, Head, Recurity Labs GmbH

Exploitation of active networking equipment has its own history and challenges. This session will take you through the full spectrum of possible attacks, what they yield and how the art of exploitation in that particular field evolved over the recent past to its present state. We will cover attacks on Cisco equipment and compare them to other specimen in the field, talk about the challenges you face to get a simple shell on such devices and what to actually do with them once you made it.

Breaking the "Unbreakable" Oracle with Metasploit

Chris Gates, Member, Metasploit Project
Mario Ceballos, Developer, Metasploit Project

Over the years there have been tons of Oracle exploits, SQL Injection vulnerabilities, and post exploitation tricks and tools that had no order, methodology, or standardization, mainly just random .sql files. Additionally, none of the publicly available Pentest Frameworks have the ability to leverage built-in package SQL Injection vulnerabilities for privilege escalation, data extraction, or getting operating system access. In this presentation we are going to present an Oracle Pentesting Methodology and give you all the tools to break the "unbreakable" Oracle as Metasploit auxiliary modules. We've created your version and SID enumeration modules, account bruteforcing modules, ported all the public (and not so public) Oracle SQL Injection vulnerabilities into SQLI modules (with IDS evasion examples for 10g/11g), modules for OS interaction, and modules for automating some of our post exploitation tasks.

Asymmetric Defense: How to Fight Off the NSA Red Team with Five People or Less

Efstratios L. Gavas, Assistant Professor, United States Merchant Marine Academy

The NSA sponsors an annual Cyber Defense Exercise (CDX) to raise awareness of and help develop cyber defense skills in our armed forces. This is the story of how the United Stated Merchant Marine Academy, the smallest of the five undergraduate service academies, has managed to hold its own, and even win one year, in head-to-head competition against other well-funded and well-organized federal academies from cyber attacks by the NSA Red Team with borrowed equipment, no funding, and no computer science program. The talk will cover thoughts on keeping your network manageable if you don't have an army of administrators and a DoD budget. We may also make fun of the Coast Guard Academy.

Locally Exploiting Wireless Sensors

Travis Goodspeed, Engineer of Superior Buckles, Goodspeed and Gourneau

Wireless sensors are often built with a microcontroller and a radio chip, connected only by a SPI bus. The radio, not the MCU, is responsible for symmetrical cryptography of each packet. When the key is loaded, it is sent as cleartext over the SPI bus, and an attacker with local access can steal the key using a few syringe probes and readily available hardware. This attack and other local attacks against wireless sensor networks will be presented in detail, including a live demo of an AES128 key being extracted from an operational network. Following the conclusion of the lecture, audience members will be brought onstage to perform the attack themselves on various pieces of example hardware.

An Open JTAG Debugger

Travis Goodspeed, Engineer of Superior Buckles, Goodspeed & Gourneau

While it's simple enough to build a "Wiggler" JTAG adapter for the PC parallel port, there is very little open hardware for performing high-speed programming of JTAG devices by USB. This lecture introduces the GoodFET, an open source USB JTAG adapter which can be reflashed to support the programming and debugging of any number of chips. Both hardware and firmware are compared to that of a similar, commercial design.

This lecture will also cover the details of the JTAG standard and a few of its competitors, as well as the possibility of attacking these debugging modes when access has been denied or restricted.

Welcome to Defcon 17 with Dark Tangent and the Making & Hacking of the DC17 Badge

Joe Grand (Kingpin) & The Dark Tangent

For the fourth year in a row, the DEFCON Badge makes its appearance as a full-fledged, active electronic system. Pushing fabrication techniques to the limit and using some components that are so new they barely exist, the design of this year's badge took some serious risks. Did they pay off? You be the judge! Every year, there are new problems and experiences to learn from and share. Join Kingpin as he guides you through the entire process of the badge, from initial concept drawings to prototype electronics to firmware design to manufacturing.

At last year's Closing Ceremonies, The Dark Tangent deemed the DEFCON Badge Hacking Contest a "black badge" event. Now, hacking the badge can earn you the ultimate in bragging rights. Kingpin will go into detail of the hackable aspects of the DEFCON 17 Badge, including setting up the development environment and using the bootloader to load your own firmware. The goal is to get people up and running faster, so they have more time over the weekend to make the badge do crazy and mischievous things. Not all the secrets of the badge will be revealed, but armed with the knowledge from this talk, you'll have a step up on the competition.

The Projects of "Prototype This!"

Joe Grand (Kingpin) & Zoz

Designing and building projects is hard. Designing and building projects of things that have never been done before is harder. Designing and building projects of things that have never been done before with the financial and time constraints of TV is ridiculous.

For 18 months, Joe Grand and Zoz were co-hosts of Prototype This! on Discovery Channel, an engineering entertainment program that followed the real-life design process of a unique prototype every episode. Comprised of an electrical engineer (Joe), a roboticist (Zoz), a material scientist, and special effects guy, we had the major bases covered. A total of thirteen episodes were produced, each with their share of challenges and drama. Sometimes the prototypes worked, sometimes they didn't.

In this mostly visual presentation, we'll go through design details and show never-before-seen pictures and videos related to some of our favorite episodes, including the Traffic Busting Truck, Fire Fighter PyroPack, Virtual Sea Adventure, Waterslide Simulator, and Flying Lifeguard, each of which had to be designed and built in a matter of weeks.

"Smart" Parking Meter Implementations, Globalism, and You (aka Meter Maids Eat Their Young)

Joe "Kingpin" Grand, Jake Appelbaum& Chris Tarnovsky

Throughout the United States, cities are deploying "smart" electronic fare collection infrastructures that have been commonplace in European countries for many years. In 2003, San Francisco launched a $35 million pilot program to replace approximately 23,000 mechanical parking meters with electronic units that boasted tamper resistance, payment via smart card, auditing capabilities, and an estimated $30 million annually in fare collection revenue. Other major cities, including Atlanta, Boston, Chicago, Los Angeles, New York, Philadelphia, Portland, and San Diego, have made similar moves.

In this session, we will present our evaluation of electronic parking meters, including smart card protocol analysis and emulation, silicon die analysis, and firmware reverse engineering, all of which aided in successful breaches.

The Year In Computer Crime Cases

Jennifer Granick, Civil Liberties Director, EFF

Its been a booming year for computer crime cases as cops and civil litigants have pushed the envelope to go after people using fake names on social networking sites (the MySpace suicide case), researchers giving talks at DEFCON (MBTA v. Anderson), and students sending email to other students (the Calixte/Boston College case). The Electronic Frontier Foundation has been front and center in these cases, either filing amicus briefs or directly representing the coders and speakers under attack. At this presentation, Jennifer Granick and other EFF lawyers fresh from the courtroom will share war stories about these cases, thereby informing attendees about the latest developments in computer security law and giving pointers about how to protect yourselves from overbroad legal challenges.

The Psychology of Security Unusability

Peter Gutmann, University of Auckland, New Zealand

Most humans have a great deal of difficulty dealing with security issues. This problem is well-known and the standard response is to blame the user, but the real problem is the fact that millennia of evolutionary conditioning has caused humans to act, and react, in predictable ways to certain stimuli and situations, to the extent that in some cases no (normal) human would respond to a security system in the way that its designers intended. This talk looks at what the field of cognitive psychology can tell us about the (often surprising) ways in which the human mind deals with computer security issues, providing insight both for defenders who need to design systems for the way that real people think rather than for an abstract ideal, and for attackers who want to exploit the weaknesses of security interfaces at the human level.

Win at Reversing: Tracing & Sandboxing Through Inline Hooking

Nick Harbour, Principal Consultant, Mandiant

This presentation will discuss a new free tool for Reverse Engineering called API Thief, the "I Win" button for malware analysis.

The unique way the tool operates will be explored as well as how it is able to provide better quality data than other tracing tools currently available. Advanced usage of the tool for malware analysis will be demonstrated such as Sandboxing functionality and a new technique for automated unpacking.

FOE: Feeding Controversial News to Censored Countries (Without Using Proxy Servers)

Sho Ho, Software Engineer, Broadcasting Board of Governors

Certain countries are banning their Internet users from accessing websites that are deemed inappropriate by their officials. News organizations' websites are commonly blocked by these countries, and there are little these organizations can do to reach their audience inside those countries. FOE is a new anti-censorship tool developed in-house by the Broadcasting Board of Governors (which oversees Voice of America, Radio Free Europe, Radio Farda, Radio Free Asia, etc.), which main goal is to create a multi-platform (including mobile) architecture that allow Internet users in censored countries to receive unbiased news.

Identifying, Exploring, and Predicting Threats in the Russian Hacker Community

Dr. Thomas J. Holt, Assistant Professor, School of Criminal Justice, Michigan State University
Dr. Max Kilger, The Honeynet Project
Dr. Debora Strumsky, The University of North Carolina at Charlotte
Dr. Olga Smirnova, The University of North Carolina at Charlotte

A great deal of research has focused on the malicious software and attack tools generated by Eastern European and Russian hacker groups. Though technical explorations provide insight into how to defend against these threats, there is still a great deal that is unknown about the social world of hackers in this part of the globe. Thus, this presentation will explore the social networks, demographic characteristics, and skills of the members of eight groups from the Eastern European and Russian hacker community using open source data, including social networking sites where they detail their personal lives, interests, and activities. The findings give significant insight into the nature of this community, including technical and university training, physical locations, and social relationships between hackers and malware writers. The network ties between skilled and unskilled hackers are explored in depth, along with ways to proactively identify the most skilled hackers using simple blog content. This presentation will benefit computer security professionals, law enforcement, and the intelligence community by identifying the social dynamics that shape the Russian hacker community.

Hardware Trojans: Infiltrating the Faraday Cage

Stephen 'afterburn' Janansky CVORG, University of Delaware
Nick Waite CVORG, University of Delaware

Last year we presented some hardware trojans as a proof of concept for side-channel data exfiltration attack. Pretty blinking lights are sweet, but this time we wanted to give the hungry crowd something more crunchy to bite into. Namely, that age-old problem of how to get data in and out of a device on a secured network, no network all, or even in a SCIF, perhaps… With some hardware voodoo, let's see what manner of electronic telekinesis we can accomplish!

p.s. Our friends who wish to remain nameless say that this is considered trivial "on the other side of the wall". Is it really? Let's see if any show up! That's right, we're laying the bait, let's play spot the fed.

Catching DNS Tunnels with AI: A Talk About Artificial Intelligence, Geometry and Malicious Network Traffic

jhind, Security Researcher

The in-depth explanation, demonstration and release of a working adaptive solution for data mining DNS tunnels from network traffic.

Attacks Against 2wire Residential Gateways

Pedro "hkm" Joaquin

Some time ago there was a vulnerability in 2wire residential routers that allowed DNS Poisoning via Cross Site Request Forgery, this was widely exploited in Mexico where this router is most commonly used.

The patch actually contained an Authentication Bypass vulnerability that made things worse, and now, after the patch got patched, there are still many public unpatched vulnerabilities that plague this device.

lar and commonly used routers in Mexico, the 2wire residential gateway.

Injectable Exploits: Two New Tools for Pwning Web Apps and Browsers

Kevin Johnson, Senior Security Analyst, InGuardians
Justin Searle, Senior Security Analyst, InGuardians
Frank DiMaggio, Security Researcher

Injectable exploits focus on the exploitation of major web flaws during penetration tests. Two new tools will be released that expand the foothold penetration testers can obtain through SQL injection and XSS flaws. These tools provide greater insight into the network hosting the web application and the networks in which the users are located. We will also discuss the live CD environment that includes both tools.

Yokoso! is an infrastructure fingerprinting system delivered via XSS attack. This project contains two different parts; the fingerprints and modules for the various browser exploit frameworks. The fingerprints identify web applications deployed in the user's network, applications such as web administration interfaces to different IT manage systems. The modules portion contains code to perform two basic attacks. The first is history browsing which determines if the user has visited the sites of interest. This reveals if the user is an administrator or power user. The second attack module within Yokoso! Initiates requests to map the infrastructure of the user's network.

Laudanum is a collection of injectable files that are prebuilt to perform various attacks within a network. These files are injected via SQL injection attacks. The individual files are placed into scheduled jobs or the web root of database servers.

This is accomplished by exploiting SQL injection flaws within the web application. Laudanum includes various attacks such as shells, proxy capabilities and data collection tools.

A major feature of both tools is their scope limiting capabilities. Many similar tools lack the capability to identify target hosts before performing exploits. Both of these tools allow a penetration tester to specify target restrictions based on external IP, internal IP, and hostname.

The final portion of the talk will cover SamuraiWTF. SamuraiWTF is a live CD environment focused on web penetration tests. It was released during DEFCON 16 and has had four new releases since that time. Both Yokoso! and Laudanum will be included on a new version of SamuraiWTF released at DEFCON this year.

Stealing Profits from Stock Market Spammers or: How I Learned to Stop Worrying and Love the Spam

Grant Jordan, WiseCrack Tools

Every time you look at your inbox, there it is… SPAM! Your penis needs enlargement, a horny single girl from Russia "accidentally" emailed you, and a former Nigerian prince knows that you're just the man to safeguard his millions. But in 2007, while still a student at MIT, one particular kind caught my eye: stock spam. Those bizarre stock market "tips" that claim you should buy a particular stock because it's "about to go through the roof!!!!" Like most people, I initially thought nothing of these ridiculous emails. That was until Kyle Vogt (now of Justin.tv) proposed the stupidest idea I had ever heard: "There has to be some way we can make money off these spammers". After trying, and failing, to prove Kyle wrong, the two of us embarked on a 4-month study into the dark depths of stock spam. In this talk, I'll explain how we went from hand-sorting tens of thousands of spam emails to developing a trading strategy able to take a piece of the spammers' profits. And how, in the process, our work produced data that disproved the results of nearly all the existing stock spam research.

Something About Network Secuity

Dan Kaminsky

Hardware Black Magic: Building Devices with FPGAs

Dr. Fouad Kiamilev, Professor, Electrical and Computer Engineering Department, University of Delaware
Rodney McGee, Researcher, Electrical and Computer Engineering Department, University of Delaware

Last year at the HHV we rolled into town full of goodies in our bags. To excite people about hardware we demoed and gave away some FPGA boards to those in attendance. We realized quickly that people didn't understand what we were talking about or giving away…but seemed to really what we call the blinky light factor. It was then that we realized that something needed to be done about this, to educate the DEFcon attendees on how easy hardware really is. Too many people treat hardware like it is black magic which only few can wield. While it may be black magic, we feel it should be available to all to use. People need to learn that this black magic can be fun, exciting and easy. So we thought up a crazy idea to help some of you out. What if we just showed you how easy it was and went through, step by step, in actually building a device?

This tutorial/demo will go through the process of showing and teaching people how easy it is to rapidly design a hardware device using an FPGA. An FPGA is basically a programmable digital circuit. It can be programmed to be almost any digital circuit you like, replacing all your 7400-series chips with one small package. Starting with nothing more than an FPGA demo-board (and little to no knowledge of hardware) the audience will see how easy it is to make a device of their own. Through the use of free software and open source code, a device can quickly be assembled and programmed in a language such as C to do exactly what the user wants. The demonstration will also show the audience how to use free IP Blocks such as those provided by the OpenCores project to build their own cool devices equipped with all the peripherals they want. We will also demonstrate how to easily use Microblaze, a microprocessor written in Verilog/VHDL. Very recently the Microblaze architecture was added into the Linux Kernel (doesn't that sound like fun?!). This tutorial will overall show people how a $100 demonstration board can be used to design things like a logic analyzer (Retail: $20,000), your own 1980's style arcade game, a simple serial UART, that Ethernet sniffer you've always been dreaming, and whatever else your mind desires. By the end, people should be armed with the knowledge they need to design their own hardware devices and have no fear about doing so.

Hack The Textbook: Introducing The Textbook Security Project

Jon R. Kibler, Chief Technical Officer, Advanced Systems Engineering Technology
Mike Cooper, Senior Security Engineer, IPC Systems

Why do we have so many software security problems? Clearly, a large proportion are caused by poorly written code. Why is our code so badly written? There are many reasons, not the least of which is that writing secure code can be a difficult task. However, the problem is compounded by most programmers having been taught insecure coding practices.

The majority of the most popular and widely used college textbooks for programming never cover any security concepts. Worse, they actually teach practices that result in insecure code. For some time now, companies trying to produce secure software have been complaining that college courses and course materials fail to prepare students to write secure code, and they are tired of having to retrain recent graduates in secure programming practices.

The insecure code problem is compounded by the fact that many of the professors and instructors who teach programming are not security experts. Even if they could identify and correct the "security bugs" in textbooks, it is difficult for them to teach what is not in the textbooks or to try to teach differently from the textbooks.

Attempts by some in the academic community to get authors and publishers to include security content in textbooks has actually been met with resistance. Many in academia believe that if there were a true need for secure software development to be taught, it would be a "self-correcting problem that would be addressed by textbook authors."

The objective of The Textbook Security Project is to publicly expose the security flaws in popular textbooks, and to encourage authors to revise their books to use secure software development practices. The immediate goal of the project is to provide lists of textbooks to be critiqued and to allow security professionals to post reviews exposing a textbook's security flaws. The project also plans to provide resources to help authors identify and correct problems in their books, and to help new authors get security right the first time. The long term goal of the project is to change security from being a subject that is taught as a senior level course, to security becoming an integral part of the entire computer science curriculum.

The Day of the Updates

Itzik Kotler, Security Operation Center Team Leader, Radware
Tomer Bitton, Security Researcher, Radware

Software updates apply patches or introduce new features to an application. In most cases, the update procedure is conducted in an insecure manner, exposing the updater to execution of malicious code or to manipulation of application data such as anti-virus signatures.

This presentation will describe in detail different application-update procedures. It will then demonstrate several techniques of update-exploitation attacks, and introduce a new tool, which leverages a man-in-the-middle technique, to build and inject a fake update reply or hijack an on-going update session.

DCFluX in: The Man with the Soldering Gun

Matt Krick "DCFluX", Chief Engineer, New West Broadcasting Systems

Is this $3.99 soldering iron any good? What about RF induction soldering irons? These questions and more will be answered when you attend this talk. Less than 1 hour will teach you soldering techniques to last a life time. For everyone from the complete novice to the advanced at home prototype engineer.

Air Traffic Control: Insecurity and ADS-B

Righter Kunkel, Security Researcher

This presentation will take a look at the Air Traffic Control (ATC) system from a pilot's view. I have found some interesting security problems with the ATC system. We will start the talk by explaining how the current ATC system works. Talk about an interesting attack vector that starts with going to a doctor to get a class 3 physical. We will talk about the future ATC system and how security may go from bad to worse. I want to open peoples eyes to the insecurity of the ATC system.

Effective Information Security Career Planning

Lee Kushner, President, LJ Kushner and Associates, Founder, InfoSecLeaders.com
Mike Murray President, Michael Murray and Associates, Founder, InfoSecLeaders.com

Even with the downturn in the economy, Information Security is becoming an increasingly popular profession. It is evident that the number of talented Information Security professionals greatly outnumbers Information Security leadership opportunities. The future will only bring fiercer competition. It is important, that you, the Information Security professional prepare yourself to compete in this employment marketplace. This interactive, half-day seminar will enable the attendee to effectively plan for future success.

Through the use of real-life experiences and guided exercises, Lee Kushner and Mike Murray, will provide a platform for the attendees to objectively evaluate their current skills and develop a long-term career strategy. Each attendee should leave with an outline for a functional career plan and recommendations on how to choose and evaluate career investments that best suit their personal objectives. At the course's conclusion, the audience will become more effective career managers and be better prepared to achieve their long term career goals.

eXercise in Messaging and Presence Pwnage

Ava Latrope, Security Consultant, iSEC Partners

eXtensible Messaging and Presence Protocol, or XMPP, is a is a set of specialized XML-based protocols that are an increasingly popular choice for a variety of middleware applications. It's a sprawling project implemented differently by many popular projects and services, and is used for purposes ranging from chat rooms and video conferencing to control channels for mobile devices. It combines a myriad of confusing buffet-style design options with all of the traditional weaknesses of XML security. XML parsing is a fragile art and many (if not most) implementations are vulnerable to DOS attacks, such as knocking the other users of a chatroom offline. I take a look at how those issues play out in IM clients and open source servers.

Picking Electronic Locks Using TCP Sequence Prediction

Ricky Lawshae, Network Technician, Texas State University

As networked building access systems become more and more popular, the security of using RFID, magstripe, and biometrics as authentication mediums is constantly under scrutiny. But what about the security of the access system itself? Is it possible to unlock a door by sending a spoofed command to it over the network, bypassing the need for an authentication medium entirely? (SPOILER ALERT: Yeah, it is.)

Perspective of the DoD Chief Security Officer

Robert F. Lentz

The last year has been a tipping point for cyber security! Safeguarding the internet and the underlying critical information infrastructures has taken center stage as a National imperative. We share threats & vulnerabilities to these fragile underpinnings critical to our ability to sustain economic growth, foster international stability and achieve national security. Do we adequately collaborate across public and private sector for protection and defense? Is our risk appetite sufficient to manage the polarity between information sharing, access, and security? And what is the Military's role in defense of our cyber national security?

Making Fun of Your Malware

Michael Ligh, Malicious Code Analyst, iDefense
Matthew Richard, Malicious Code Operations Lead, Raytheon Corporation

Would you laugh if you saw a bank robber accidentally put his mask on backwards and fall into a man hole during the getaway, because he couldn't tell where he was going? Criminals do ridiculous things so often, its impossible to capture them all on video. Rest assured, when the criminals are malware authors, we can still make fun of them through evidence found in pictures, binary disassemblies, packet captures, and log files. This talk evenly distributes technical knowledge and humor to present the funniest discoveries related to malware authors and the fight against their code.

Abusing Firefox Addons

Roberto Suggi Liverani, Senior Security Consultant, Security-Assessment.com
Nick Freeman, Security Consultant, Security-Assessment.com

Hundreds of Firefox addons are created every week. Millions of users download them. Some addons are even recommended by the Mozilla community, and users implicitly trust them. We don't trust a single one, and we will show you why.

This talk details how we have abused some of the most popular and recommended Firefox addons, with previously unreleased vulnerabilities. From the Mozilla download statistics, over 15 million users are potentially affected. Demos will cover remote code execution, local file disclosure and other tailored Firefox Addon exploits.

Don't panic—the Addons manager can be found under the 'Tools' tab in your Firefox menu. We expect to see a lot of people clicking the "Uninstall" button after this presentation.

DC Network Session

Lockheed Sr. Goon, DefCon Network Operations Group

For years, the inner-workings of the DefCon NOC were kept under wraps. Last year Wired was allowed a sneak-peak inside. This year at DefCon17 we are opening the kimono. In true open-source style, we are holding a peer-review discussion session. We will be showing you how the DefCon NOC operates, how the network is laid out, designed, what it is we do. This is not a typical lecture-style talk, but instead intended to be an interactive session, which is why we've arranged to hold it in the more intimate setting. We often get people interested in participating as part of the team - this is our way of opening up and allowing you to have a chance to review the network, make suggestions, tell us where you think we could improve upon things, and make your own contribution to DefCon!

Jailbreaking and the Law of Reversing

Fred Von Lohmann, Senior Staff Attorney, EFF
Jennifer Granick, Civil Liberties Director, EFF

Using jailbreaking of the iPhone as a primary example, the presentation will be an overview of the laws relating to reverse engineering of hardware and software.

Developers who rely on reverse engineering face a thicket of potential legal obstacles, including license agreements, copyright, the Digital Millennium Copyright Act (DMCA), and the Computer Fraud and Abuse Act

(CFAA). Taking iPhone jailbreaking as real-world example, we will review the legal theories Apple has asserted, shedding light on the major legal pitfalls that developers face, and what they can do to avoid them and minimize risks. We will also examine the additional legal issues raised by reverse engineering networked code, such as online video games.

The presentation stems from the presenters' experience as attorneys with EFF's "Coder's Rights Project," as well as their efforts to persuade the U.S. Copyright Office to grant a DMCA exemption for removing application locks on smartphones (including the iPhone and Android G1).

three point Oh.

Johnny Long, Co-Pilot, Hackers For Charity

From scrubby C64 pirate to professional hacker to reluctant "Internet rockstar", the past five years of Johnny's journey have been interesting. The last few months, however, have been straight-up bizarre.

While many strain to maintain and others scrape and scratch at the ladder, Johnny's jumped off the top rung.

This is a story of what it takes to make it in this industry, and what the view's like from the top.

This is a story about how utterly teh suck the view from the top really is and why you might want to just jump off now before it's too late.

This is the story of a rise and fall and the crossover cable those terms require.

This is a story that's relevant if you're in for the long haul.

This is Johnny's story, as only Johnny can tell it.

Which means it might be funny.

Hack like the Movie Stars: A Big-Screen Multi-Touch Network Monitor

George Louthan, Research Assistant, University of Tulsa
Cody Pollet, Research Assistant, University of Tulsa

You know all those movies where exaggerated nerd-types accomplish impossible hacking feats using a ridiculous, big-screen friendly, animated graphical interface where they appear to fly through the network, performing complicated tasks with the flick of their finger? You thought to yourself, "Wow, that's impractical and useless". But somewhere, deep down, some part of you thought it was pretty sweet. That's why we built one. We call it DVNE.

We'll be presenting a prototype rear-projection multi-touch interface for exploring and interacting with networks backed by a signature-based network monitor. We'll talk about the technology behind multi-touch, our network monitor, and some of the shiny but totally impractical features we're incorporating. And, assuming the airlines cooperate, we'll be running a live demo as well.

Is your Iphone Pwned? Auditing, Attacking and Defending Mobile Devices

Kevin Mahaffey ,co-founder and CTO, Flexilis
John Hering, co-founder, Flexilis Mobile Security
Anthony Lineberry, Security Researcher

The world has never been more connected. Over a billion mobile devices ship every year, five times the number of PCs in the same period. The iPhone and Android have accelerated the mass adoption of smart devices, mobile applications, and high speed mobile networks. Meanwhile, mobile devices are now a material target: they contain sensitive personal and corporate data, access privileged networks, and routinely perform financial transactions. The question remains, how do we keep these devices safe?

Learn about how to detect vulnerabilities on mobile devices, exploitation techniques, how the security architecture of major mobile platforms work, and how to protect your mobile device(s) in the threat landscape of a constantly evolving mobile world. We'll be demonstrating a new mobile device vulnerability (we're also providing a hotfix tool) and analyzing other vulnerabilities that affect major mobile platforms, one of which is already being actively exploited in the wild. To top it off, we will be releasing our 'Sniper' mobile fuzzing framework, a tool specifically designed to fuzz mobile platforms that includes support for major file formats and protocols typically present on mobile devices.

Hacking the Wiimote and Wii Fit to Help the Disabled

Josh Marks, Rob Rehrig & Larry Aiello

People like Johnny Chung Lee have shown us that the Wiimote can be used as a bluetooth IR camera that tracks the spatial location of up to four IR LEDs. Applying this work to a new application, we have adapted the Wiimote and the Wii Fit into a low cost system to help disabled individuals to interface with a computer. By combining the movement of head mounted LEDs and measurement of weight distribution of the lower body (ie "butt-movement"), users are able to provide input gestures. The system uses the gesture recognition engine originally designed by makers of the iPhone.

Our setup can also be used by normal individuals for a heightened gaming experience. This talk will feature a live demonstration of the interface and uses of the hardware. The only question that remains is "Would you like to play a game?".

More Tricks For Defeating SSL

Moxie Marlinspike

This talk aims to pick up where SSL stripping left off. While sslstrip ultimately remains quite deadly in practice, this talk will demonstrate some new tricks for defeating SSL/TLS in places where sslstrip does not reach. Cautious users, for example, have been advised to explicitly visit https URLs or to use bookmarks in order to protect themselves from sslstrip, while other SSL/TLS based protocols such as imaps, pop3s, smtps, ssl/irc, and SSL-based VPNs never present an opportunity for stripping. This talk will outline some new tools and tricks aimed at these points of communication, ultimately providing highly effective attacks on SSL/TLS connections themselves.

Advanced SQL Injection

Joseph McCray Founder of Learn Security Online

SQL Injection is a vulnerability that is often missed by web application security scanners, and it's a vulnerability that is often rated as NOT exploitable by security testers when it actually can be exploited.

Advanced SQL Injection is a presentation geared toward showing security professionals advanced exploitation techniques for situations when you must prove to the customer the extent of compromise that is possible.

The key areas are:

- IDS Evasion, Web Application Firewall Bypass
- Privilege Escalation
- Re-Enabling stored procedures
- Obtaining an interactive command-shell
- Data Exfiltration via DNS

Joseph McCray has 8 years of experience in the security industry with a diverse background that includes network and web application penetration testing, forensics, training, and regulatory compliance. Joe is a frequent presenter at security conferences, and has taught the CISSP, CEH, CHFI, and Web Application Security at Johns Hopkins University (JHU), University of Maryland Baltimore College (UMBC), and several other technical training centers across the country.

Clobbering the Cloud

Haroon Meer, Technical Director, SensePost
Marco Slaviero, Cyber Fighter, SensePost
Nicholas Arvanitis, Senior Security Analyst, SensePost

Cloud Computing dominates the headlines these days but like most paradigm changes this introduces new risks and new opportunities for us to consider. Some deep technical research has gone into the underlying technologies (like Virtualization) but to some extent this serves only to muddy the waters when considering the overall threat landscape. During this talk SensePost will attempt to separate fact from fiction while walking through several real-world attacks on "the cloud". The talk will focus both on attacks against the cloud and on using these platforms as attack tools for general Internet mayhem. For purposes of demonstration we will focus most of our demos and attacks against the big players…

Managed Code Rootkits: Hooking into Runtime Environments

Erez Metula, Application Security Department Manager, 2BSecure

This presentation introduces a new concept of application level rootkit attacks on managed code environments, enabling an attacker to change the language runtime implementation, and to hide malicious code inside its core. Taking the ".NET Rootkits" concepts a step further, while covering generic methods of malware development (rootkits,backdoors,logic manipulation, etc.) for the .NET framework and Java's JVM, by changing its behavior. It includes demos of information logging, reverse shells, backdoors, encryption keys fixation, and other nasty things.

This presentation will introduce the new version of ".Net-Sploit" - a generic language modification tool, used to implement the rootkit concepts. Information about .NET modification - The Whitepaper, .NET-Sploit, and source code can be found here:

http://www.applicationsecurity.co.il/.NET-Framework-Rootkits.aspx

Subverting the World Of Warcraft API

Christopher Mooney, Software Engineer, Project DoD
James Luedke, Software Engineer, Project DoD

The authors will demonstrate how to work within the World of Warcraft API framework to re-enable the features of protected and disabled functions. They will explain their library and how to use it to get around the restrictions on programmatically casting spells, targeting, moving, and performing those actions in response to UI events. What's more, they will use this library to do a live demonstration of this code autonomously playing battlegrounds. This talk will include a description of how their library works with example source, how you can download and use the code, and how to get involved with the community developing this code. All tools will be released the day of the talk, and source will be release under the GPL3 license. In true DEFCON fashion the authors will talk about the problem they were trying to solve, demonstrate the break on the security system, demonstrate the code in action, and release the tools. If you're a hacker, you're going to love this talk. If you're a developer, you're going to love this talk. If you're a gamer, your going to love this talk. If you're a hacker, a developer, and a gamer, you cannot afford to miss this.

Defcon Security Jam 2: The Fails Keep on Coming

David Mortman, CSO in Residence, Echelon One
Rich Mogull, Securosis
Dave Maynor, Founder & CTO Errata Security
Larry Pesce, Paul.com
Robert "RSnake" Hansen, ha.ckers.org

We're baaaack. Yup that's right, some of the biggest mouths in Information Security and once again, we will show you all new of security FAIL. Our panelists will demonstrate innovative hacking techniques in naked wireless networking, GPS, intranet routing, web based applications and goats.

RAID Recovery: Recover your PORN by Sight and Sound

Scott Moulton, System Specialist, Forensic Strategy Services

This talk will focus on RAID reassembly. In both Forensics and Data Recovery it is common for there to be PORN not only in Pictures but also in Sound Files and Video Files. The goal is $100 or less, figure out how to reconstruct RAID 0 and RAID 5 arrays using the PORN on the array to help identify the correct order of the drives and the variations in the slice size. This is a demo of how to use those files to figure out the layout for the RAID and how to find the right configuration when it is unknown using PORN.

Weaponizing the Web: New Attacks on User-generated Content

Shawn Moyer & Nathan Hamiel

Ultimately, basing the value proposition of your site on user-generated and external content is a kind of variant on Russian Roulette, where in every turn the gun is pointed at your head, regardless of the number of players. You may win most of the time, but eventually a bullet is going to find its way into the chamber with your name on it.

We spent some time last year looking at this problem as it related specifically to Social Networks, but that left a lot of the territory unexplored. This time around we'll be talking about a previously unnoticed attack vector for lots and lots of web applications with user-generated content, and releasing a handy tool to exploit it. Bundled in are some thoughts on Web 2.0 attack surface, a few new exploitation techniques, and as in last year, a hefty helping of lulz, ridicule, and demos-of-shame at the expense of a few of your and (our) favorite sites.

Slight of Mind: Magic and Social Engineering

Mike Murray, VP, Foreground Security
Tyler Reguly, Sr. Security Research Engineer, nCircle Network Security

Magicians are the ultimate social engineers; they take something completely untrue and make it believable to an audience sometimes numbering in the millions. In a presentation befitting the Vegas audience, three security professionals who study magic and social engineering will present a combination of entertainment and lecture that will teach the audience some of the themes of stage magic that can be applied to social engineering engagements.

Hacking Sleep: How to Build Your Very Own Sleep Lab

Ne0nRa1n, Researcher
Keith Biddulph, Researcher

What is sleep? What happens when we don't get enough of it? Can it be hacked? Now that electronics are cheaper and more portable than ever before, a new generation of hackers have found themselves with the ability to build their own machines to measure and analyze the human body in ways only available to universities and hospitals in the past. This presentation will cover some current theories on the science of sleep and sleep disorders, as well as explain how to build your own home-brew sleep lab and read the data that you'll collect from it.

Advancing Video Application Attacks with Video Interception, Recording, and Replay

Jason Ostrom, Director, VIPER Lab Sipera Systems
Arjun Sambamoorthy, Research Engineer, Sipera Systems

New video applications promise many exciting cost-saving benefits, but they also bring with them a host of security challenges and vulnerabilities. This session applies existing techniques for VoIP eavesdropping towards next generation attacks against Unified Communication technologies, such as intercepting and recording private video conferences, IP video surveillance systems, and other video collaboration technology. This presentation will focus primarily on informative and insightful live demos that show targeted video attacks and issues that put video application traffic at risk. We will focus on the following:

- First public demonstration of a new version of UCSniff 3.0, a Windows port of the code, with enhanced video eavesdropping features.
- A new version of a second free assessment tool, "VideoJak," with two new video exploits.
- A new free assessment tool, videosnarf, which takes an offline pcap as input, and outputs any detected video streams into separate avi video files.
- A surprise tip that we have learned through VoIP pentesting of production enterprise networks. .

Note that all the tools to be demonstrated are open source, available to the security community at large and that we do not distribute them in any commercial way.

RFID MythBusting

Chris Paget, Founder, H4RDW4RE

This presentation is about challenging many of the popular preconceptions about RFID technology. "Short-range" will be shot down first (I'm aiming to set a half-mile world record in the Nevada desert just before Defcon), "secure" will be busted second (don't bring _any_ RFID tags unless you want them cloned), "immune to electromagnetic pulse weaponry" will fall last (and hopefully most spectacularly). I'll be covering a wide range of different RFID technologies from 125KHz to 900MHz, and releasing a whole pile of source code, schematics, and (with luck) a little magic smoke.

Undeterred by his previous legal skirmishes, Chris Paget is still having fun playing with magnetic fields and RFID. If you see a tall guy wandering around the con with long hair, high heels, and a pile of home-made RF hardware, there's a good chance that a) it's him, and b) your RFID cards have just been cloned.

Malware Freak Show

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

We see a lot of compromised environments every year. In 2008 alone, we performed full forensic investigations on over 150 different environments ranging from financial institutions, hotels, restaurants and even some casinos not too far from DEFCON. This presentation will show the inner workings of three very interesting pieces of malware, ranging from somewhat simple to very complex. Each sample was actually used to steal confidential data that resulted in significant fraud and business loss for the organizations we found them at. Many of the pieces of malware we have been running across are very advanced pieces of software written by very skilled developers. The complexity in their propagation, control channels, and data exporting properties will be very interesting to anyone interested in this topic.

Introduction to WiMAX Hacking

Goldy & Pierce

WiMAX is a new high speed, 802.16e, wide area broadband service that promises to replace 3G high speed networks. It is only being offered in a few cities across the country, but by 2012 it is estimated that it will be nation wide. Over the last decade, hackers have explored and demonstrated weaknesses in the security of WiFi, pushing the industry to come up with better security practices. In this talk, we intend to make it clear what WiMAX is, what is being done to protect the existing deployed WiMAX networks, and different ways to get anonymous Internet anywhere WiMAX is being served.

Search And Seizure Explained - They Took My Laptop!

Tyler Pitchford, Esq., CTO, Digome

An overview of recent developments surrounding the Fourth and Fifth Amendments of the United States Constitution and their impact upon privacy conscious computer professionals. The presentation includes discussions on the United States Constitution, Federal Statutes, Administrative decisions, and, most importantly, the case laws that interpret and define the Fourth Amendment and Fifth Amendments. Special attention is given to topics affecting computer professionals, including border crossings, foreign nationals, encryption, forced disclosures, the Crist decision, and the Boucher decisions.

Fragging Game Servers

Bruce Potter, Founder, The Shmoo Group
Logan Lodge, TFT Ninja

Every day, security professionals do battle the trenches; good vs. evil, whitehats vs. blackhats, our network vs their l337 tools. And what do we do to unwind after work? For many of us, it's doing battle in the trenches with terrorists, Nazi's, and that pesky Blue team that keeps stealing our intelligence.

Video games are a multi-billion dollar industry that rivals the movie industry in size. And recently, many games have taken a decidedly online tone. People from all over the world meet up on servers every day to meet, frag, and respawn into the wee hours of the morning. But what about the security of these servers? How secure are they, and how does the underlying integrity of these servers effect you and your ability to blow up other players?

From hardware interaction to network protocols, this talk will present the inner workings of the Source Dedicated Server (used for games such as Left4Dead and Team Fortress 2). This talk will discuss some of the weaknesses in these game engines and ways they are exploited in the wild. A tool designed to dissect and analyze client/server communications will be released during the talk. We'll also provide some pragmatic advice for deploying game servers and release a white paper describing a secure configuration guidelines for the Source Dedicated Server.

Smashing the Stack with Hydra: The Many Heads of Advanced Polymorphic Shellcode

Pratap Prabhu Research Assistant, Columbia University
Yingbo Song Research, Assistant, Columbia University
Salvatore. J. Stolfo, Professor of Computer Science, Columbia University

Recent work on the analysis of polymorphic shellcode engines suggests that modern obfuscation methods would soon eliminate the usefulness of signature-based network intrusion detection methods and supports growing views that the new generation of shellcode cannot be

accurately and efficiently represented by the string signatures which current IDS and AV scanners rely upon. In this presentation, we expand on this area of study by demonstrating never before seen concepts in advanced shellcode polymorphism with a proof-of-concept engine which we call Hydra. Hydra distinguishes itself by integrating an array of obfuscation techniques, such as recursive NOP sleds and multi-layer ciphering into one system while offering multiple improvements upon existing strategies. We also introduce never before seen attack methods such as byte-splicing statistical mimicry, safe-returns with forking shellcode and syscall-time-locking. Multi-tasking shellcode with safe-returns ensures that we bypass sensors that monitor application crashes. Also, we bypass online emulators by deriving an encryption key from the OS environment—something that is not easy to implement in an emulator. In total, Hydra simultaneously attacks signature, statistical, disassembly, behavioral and emulation-based sensors, as well as frustrates offline forensics. This engine was developed to present an updated view of the frontier of modern polymorphic shellcode and provide an effective tool for evaluation of IDS systems, Cyber test ranges and other related security technologies.

Maximum CTF: Getting the Most Out of Capture the Flag

Psifertex

Among all the amazing Defcon competitions, the Capture the Flag contest reigns supreme. Psifertex will examine some of the history of CTF, focusing on the reign of terror pwnage that was the Kenshoto CTF from 2005-2008. The talk will both be technical (including rapid-fire discussions of technical challenges and solutions), and entertaining (expect guest appearances from ninjas and pirates alike). Come hear not only what skills are necessary to succeed at CTF, but how to have the most fun while doing it.

Reverse Engineering By Crayon: Game Changing Hypervisor Based Malware Analysis and Visualization

Danny Quist CEO, Offensive Computing
Lorie M. Liebrock, New Mexico Tech Computer Science Department

Recent advances in hypervisor based application profilers have changed the game of reverse engineering. These powerful tools have made it orders of magnitude easier to reverse engineer and enabled the next generation of analysis techniques. We will also present and release our tool VERA, which is an advanced code visualization and profiling tool that integrates with the Ether Xen extensions. VERA allows for high-level program monitoring, as well as low-level code analysis. Using VERA, we'll show how easy the process of unpacking armored code is, as well as identifying relevant and interesting portions of executables. VERA integrates with IDA Pro easily and helps you to annotate the executable before looking at a single assembly instruction. Initial testing with inexperienced reversers has shown that this tool provides an order of magnitude speedup compared to traditional techniques.

Automated Malware Similarity Analysis

Daniel Raygoza, DC3, General Dynamics

While it is fairly straightforward for a malware analyst to compare two pieces of malware for code reuse, it is not a simple task to scale to thousands of pieces of code. Many existing automated approaches focus on runtime analysis and critical trait extraction through signatures, but they don't focus on code reuse. Automated code reuse detection can help malware analysts quickly identify previously analyzed code, develop links between malware and its authors, and triage large volumes of incoming data.

Injecting Electromagnetic Pulses into Digital Devices

Paul F. Renda, Data Security Analyst, Futurist

This talk is not about someone on the ground firing a ray gun at a jet and bringing it down, this talk is about someone on the jet injecting EMP in the wiring system of the jet and causing great problems with the aviation systems and the black box. I will define smart and dumb digital devices based to how they respond to injected pulses. The talk will have at least 10 video demos of device pulses and a video of a surge protector. The Marx generator will be explained and a mosfet charging circuit. Going green, fly by wire airplanes, robotic control trains, densely integrated systems, these are all realities of our daily environment. One problem is that all of these make our life more susceptible to an EMP disruption. Other topics covered include TWA 800, Telsa coil, Byzantine faults and the power grid. Note : Contact me if you live in the northeast and have a pole pig I can rent for 2 hours.

Hacker vs. Disasters Large and Small: Hacker Skills for Wilderness and Disaster Survival (Part 1)

RenderMan
Michael "theprez98" Schearer

Part 1: Our hacker brains are pre-wired to find alternate uses for many devices, but most often we're "on the grid" and close to our precious electronics and high speed internet. What would happen if you find yourself stranded in the middle of nowhere, become lost during a simple daytime hike, or wake up in the midst of a natural disaster? Over the past year, I have gone to "the middle of nowhere" armed with my video camera, a la survivorman, to demonstrate how your hacker skills are largely compatible with the skills necessary to survive in the wilderness or during a natural disaster. Using demonstrations of simple techniques, some ancient and others more modern, this presentation will show you that your hacker ingenuity is well-suited to helping you survive the worst.

Part 2: Large Scale Emergency and Disaster Survival

RenderMan

Introduction: We as hackers are a unique breed of human. We look at the world as a puzzle to solve in everything we do. We can come up with the most extraordinary solutions to problems under the most extraordinary circumstances. However though, we are the first to admit that without technology, many of us are rather useless. Do we have what it takes to think outside the box if the internet and technology suddenly went away? Society in general is becoming more and more dependent on technology, what skills are likely to be missing or forgotten in the event of a major cataclysm? Many of us could survive for short term disasters, but what about long term, society rebooting events? Could we be useful in rebuilding society by taking steps to preserve useful knowledge?

So You Got Arrested in Vegas...

Jim Rennie, Attorney

Vegas is all fun and games until someone gets arrested. Do you know what to do if you or your buddies get thrown in the slammer? Want to get the heck out of there before its time for your flight home? If so, then this talk is for you. Come find out how much trouble you might get into while you're here. Find out the locations of the local jails. Understand the process of being taken into custody and bailing out again. Pick up a handy card that has valuable contact information should someone spend the night in the slammer! Sure, you may laugh now, but just wait until you're in the holding tank with 10 other DefCon attendees.

0-day, gh0stnet and the Inside Story of the Adobe JBIG2 Vulnerability

Matt Richard, Malicious Code Researcher, Raytheon
Steven Adair, Researcher, Shadowserver

This talk is the story of 0-day PDF attacks, the now famous gh0stnet ring and the disclosure debacle of the Adobe JBIG2 vulnerability in January and February 2009. This is the story of international cyber-espionage using 0-days and the fierce debate over how to defend networks in the face of prolonged periods of exposure to unpatched vulnerabilities.

We seek to answer the following questions in this talk:

- Who was behind the early 0-day attacks and are they the same as the gh0stnet report published in April 2009?
- Did disclosure of the Adobe JBIG2 vulnerability have an impact on targeted attacks?
- How effective were post-disclosure protections such as AV signatures, IDS signatures and workarounds?

Throughout the talk we dissect the 0-day artifacts and other events leading up to the partial disclosure of the JBIG2 vulnerability on February 19 by ShadowServer. Using a variety of 0day PDF samples we will analyze the 0-day attacks and attempt to correlate them to the attackers discussed in the recent paper "Tracking GhostNet: Investigating a Cyber Espionage Network".

We will also look at the partial disclosure by ShadowServer and then full disclosure on the Sourcefire blog and assess the impact on targeted attacks. We will analyze the various malicious PDF's submitted to Virustotal to determine their lineage and relationship to either the original 0day exploit and gh0stnet or new attacks that sprang up in the wake of the disclosure. The analysis tools and techniques will be shared to aid future analysis efforts.

Hackerspaces: The Legal Bases

Nicolle Neulist "RogueClown"

Hacker communities in many cities are becoming interested in starting hackerspaces. Getting together a core of talented, inquisitive, and creative people is an integral part of it, but it is also important to address the legal questions that arise. The goal of this presentation is to make anyone interested in hackerspaces aware of the most likely legal issues to arise, and to equip them to ask the right questions. The subjects discussed in the presentation include choosing an organizational structure, specific benefits and concerns that arise if a hackerspace is organized as a nonprofit, zoning and leasing issues that arise when finding a physical space, and managing liability in order to protect officers, directors, members, and guests alike.

The Security Risks of Web 2.0

David Rook

Web 2.0 technologies are changing the landscape of the Internet by delivering significant increases in the functionality of websites and providing a more interactive experience to the user. This rapid proliferation of new technologies is also accompanied by new attack vectors that hackers are eager to exploit. I will detail the security risks introduced by web 2.0 and how you can prevent them.

Deblaze: A Remote Method Enumeration Tool for Flex Servers

Jon Rose, Trustwave

This talk will provide a basic overview of Flash remoting and cover some of the security issues found in real-world flash applications and demonstrate a new tool for testing flash applications.

Flash applications can make request to a remote server to call server side functions, such as looking up accounts, retrieving additional data and graphics, and performing complex business operations. However, the ability to call remote methods also increases the attack surface exposed by these applications. Deblaze came about as a necessity during a few security assessments of flash based websites that made heavy use of flash remoting. I needed something to give me the ability to dig a little deeper into the technology and identify security holes. This tool will allow you to perform method enumeration and interrogation against flash remoting end points.

The latest version can be found at deblaze-tool.appspot.com

Protecting Against and Investigating Insider Threats (A methodical, multi-pronged approach to protecting your organization)

Antonio "Tony" Rucci, Program Director, Technical Intelligence and Security Programs, Oak Ridge National Laboratory

This presentation will focus on indicators of insider threats and how to detect them. I'll primarily focus on specific hiring practices to minimize risk to your organization. We'll take a deep dive look into open source searches you should be doing on the internet that may expose someone who could potentially be a liability to you and your company. I'll talk about the importance of security awareness training and education to thwart opportunistic individuals. And Finally, we'll wrap things up with some interesting, relevant case studies that illustrate the key indicators and what their status is today.

Failure

Adam Savage, Co-Host, MythBusters

A meditation on how I've screwed things up, lost friends and clients, and learned about myself in the process.

Cloud Security in Map/Reduce

Jason Schlesinger, Security Researcher

This presentation is an overview of the operations principles of Map/Reduce and Hadoop with examples of typical implementation in a business environment. It points out significant security issues that now exist and others that will certainly arise. The presentation also offers suggestions for improving security in existing installations, and presents improvements to provide security going forward.

Q & A with Bruce Schneier

Bruce Schneier is an internationally renowned security technologist and CTO of BT Counterpane, referred to by The Economist as a "security guru." He is the author of eight books—including the best sellers "Beyond Fear: Thinking Sensibly about Security in an Uncertain World," "Secrets and Lies," and "Applied Cryptography"—and hundreds of articles and academic papers. His influential newsletter, Crypto-Gram, and blog "Schneier on Security," are read by over 250,000 people. He is a prolific writer and lecturer, a frequent guest on television and radio, has testified before Congress, and is regularly quoted in the press on issues surrounding security and privacy.

Screen Scraper Tricks: Extracting Data from Difficult Websites

Michael Schrenk

Screen scrapers and data mining bots often encounter problems when extracting data from modern websites. Obstacles like AJAX discourage many bot writers from completing screen scraping projects. The good news is that you can overcome most challenges if you learn a few tricks.

This session describes the (sometimes mind numbing) roadblocks that can come between you and your ability to apply a screen scraper to a website. You'll discover simple techniques for extracting data from websites that freely employ DHTML, AJAX, complex cookie management as well as other techniques. Additionally, you will also learn how "agencies" create large scale CAPTCHA solutions.

All the tools discussed in this talk are available for free, offer complete customization and run on multiple platforms.

That Awesome Time I Was Sued For Two Billion Dollars

Jason Scott, Textfiles.com

In a world where scams are now considered as commonplace as functioning websites and cell phones, it's sometimes too easy to forget the insidiousness and complicated preparation that can go into a well-honed misleading attempt to gain financially from unknowing people. It also helps if you're this side of crazy. For over a decade, Jason Scott (and a group of others) were plagued by one such artist of misdirection, and he will present an dismaying, tragic, but hilarious recounting of what he learned along the way and what you yourself might find yourself confronted with as you go about your business. The story is true, the two billion dollars was demanded but not awarded, and the case got to court. Come hear a legal yarn with a side order of fried conspiracy theory, and walk away a little wiser.

The Making of the Second SQL injection Worm

Sumit Siddharth, IT Security Consultant

The "turbo" talk will focus on exploiting SQL injections in web applications with oracle back-end. Mostly exploiting Oracle sql injections in web applications is considered to be restricted to extraction of data only. Oracle database does not offer hacker friendly functionalities such as openrowset or xp_cmdshell for privilege escalation and O.S code execution. Further, as web API do not support execution of multiple query in single statement, the exploitation is further restricted. The Talk will highlight attack vector to achieve privilege escalation (from Scott to SYS) and O.S code execution by exploiting Oracle SQL injections in web applications. Further, there will be demo of how a worm could target an Oracle back-end just as it targeted the SQL server applications.

Manipulation and Abuse of the Consumer Credit Reporting Agencies

Anonymous Speaker

This talk will present a number of loopholes and exploits against the system of consumer credit in the United States that can enable a careful attacker to hugely leverage her (or someone else's) credit report for hundreds of thousands of dollars. While the techniques outlined in this talk have been used for the personal (and legal) profit by a small community of credit hackers, these same techniques could equally be used by more nefarious persons { that is, criminals willing to break the law, engage in fraud, and make off with large sums of money. The purpose of this talk is to shed light on these exploits, to analyze them through the lens of the computer security community and to propose a number of fixes which will significantly reduce the effectiveness of the exploits, by both those with good and ill intentions.

Bluetooth, Smells Like Chicken

Dominic Spill, Security Researcher
Michael Ossmann, Wireless Security Researcher
Mark Steward, Security Researcher

Bluetooth traffic analysis is hard. Whilst most 802.11 chips support promiscuous mode, Bluetooth dongles cannot monitor all traffic due to a pseudo-random frequency hopping system. Previous attempts have recovered a small number of channels using software radio techniques but have required expensive equipment.

We will review the options available today for passive Bluetooth monitoring with an emphasis on software radio techniques. Although single channel monitoring with software radio has been demonstrated before, we will show how to extend the technique to all 79 channels and how to predict the target network's pseudo-random hopping sequence using passively collected information. We will also discuss the options available when a high end software radio device cannot be used and will show what we are currently able to achieve with off the shelf hardware for under $10. The presentation will feature live demonstrations of the current status of the gr-bluetooth project and a new release of the open source tools.

"I Am Walking Through a City Made of Glass and I Have a Bag Full of Rocks" (Dispelling the Myths and Discussing the Facts of Global Cyber-Warfare)

Jayson E. Street, CIO, Stratagem 1 Solutions

<hype> There is a war being raged right now. It is being fought in your living room, in your dorm room even in your board room. The weapons are your network and computers and even though it is bytes not bullets whizzing by that does not make the casualties less real. We will follow the time line of Informational Warfare and its impact today. We will go deeper past the media hype and common misconceptions to the true facts of what's happening on the Internet landscape. You will learn how the war is fought and who is fighting and who is waiting on the sidelines for the dust to settle before they attack. </hype>

We will discuss in a logical manner what is really going on as it relates to Cyber-Warfare. The answers and the questions raised will surprise you!

Dangerous Minds: The Art of Guerrilla Data Mining

Mark Ryan Del Moral Talabis, Senior Consultant, Secure-DNA Consulting

It is not a secret that in today's world, information is as valuable or maybe even more valuable that any security tool that we have out there. Information is the key. That is why the US Information Awareness Office's (IAO) motto is "scientia est potential", which means "knowledge is power". The IAO just like the CIA, FBI and others make information their business. Aside from these there are multiple military related projects like TALON,ECHELON, ADVISE, and MATRIX that are concerned with information gathering and analysis.

The goal of the Veritas Project is to model itself in the same general threat intelligence premise as the organization above but primarily based on community sharing approach and using tools, technologies, and techniques that are freely available.

The combination of all the techniques presented in this site is what we call "Guerrilla Data Mining". It's supposed to be fast, easy, and accessible to anyone. The techniques provides more emphasis on practicality than theory. For example, these tools and techniques presented can be used to visualize trends (e.g. security trends over time), summarize large and diverse data sets (forums, blogs, irc), find commonalities (e.g. profiles of computer criminals) gather a high level understanding of a topic (e.g. the US economy, military activities), and automatically categorize different topics to assist research (e.g. malware taxonomy).

People's Choice:
Watchmen Parody by Mar

T-shirt Category:
Floppy by JesseK

Poster Category:
DEFCON 17 by Steve Andrus

Bumper Sticker Category:
Tailing The Elite Hacker by downtownDB

Congratulations to the winners of the Artwork Contest. Thank you to all of the entrants for their great work!

artwork contest

Hacker Jeopardy

Rounds 1 & 2 Friday at 21:00 in Track 2 • Rounds 3 & 4 Saturday at 21:00 in Track 2

Hacker Jeopardy, Def Con's, biggest, first and longest game is back! Join 2,000+ of your fellow DefConners to watch contestants be humiliated, drink, answer really tough geeky questions, drink, sell their clothing for points, drink, and try to calculate long Hex, ASCII and Port Math questions while drinking. It starts, as usual, at 21:00 on Friday night for two games where the teams (of up to three people each) fight it out, duke it out and drink it out with questions to our answers. 21:00 on Saturday brings Round 3 and the Final between the first three games' winners. Winners get awesome stuff from DT... like Black Badges! And more. Losers get to drink. Audience Drinks. All players drink. (>21 Only). Hacker Jeopardy is rated Heavy-R. You are warned—but we have to be somewhat cool in the Riv cause it's a casino hotel.

WHO CAN PLAY? Most people play pretty lousy, but you can still try. Submit your teams to HackerJeopardy@Gmail.Com or at the Info Booth at the con and you're in the running. One year a secret government group got so drunk, they didn't answer one question right. That was humiliating. For them.

AUDIENCE PLAYS: Yup! You get to play, too. DefCon ends up with tons of swag that we toss out to audience members who come up with the right questions, we got to get rid of all this stuff,one year we gave away a couple dozen Sun workstations! Plus, you can make fun of the contestants on stage. Be rowdy. A little rowdy, not a lot rowdy. Don't want anyone arrested again for being TOO rowdy.

Social Engineering Contest

Contest Area • See Schedule at defcon.org for times

Moose of DC718, NotKevin of 2600 Magazine, and Rodent from Telephreak are bringing Social Engineering back to DefCon. HOPE and other conferences have been doing this successfully with a lot of participation for years, NotKevin has years of experience organizing this at HOPE, and we felt that this was a contest that after so many years should come back to the our conference. Thanks to this elite team up of our team with Offensive-Security, the contest/event Goons Pyr0 and Russr, and www.social-engineering.org, we have the best of the best to judge and help mold this contest into the display of the serious threat that still exists via this type of attack. Consisting of two rounds, teams will compete for the bragging rights of "Best Social Engineer @ DefCon 17, 2009." and FREE Pentesting with BackTrack certification and training from Offensive-Security for the winning team. With a few simple rules, the Social Engineering contest is open to any form, style and exploit you wish to bring, in so long as you can follow the rules and not endanger or disseminate anyone's credentials or personal information. Winners will be picked based on our judges scores. Moose and DC718 would like to thank Russr, Pyr0, Roamer, Nikita and Neil, Vegas 2.0 and Hackajar, Skydog and Lady Merlin and the whole HC crew, DT, MAFCORP and Kev, DC949, OffSec, GM1, Shmoo's around the world, and all of the Goons for taking their time all year making the conference even better every year. NotKevin and Telephreak thanks Beave, r0d3nt, Jfalcon , Droogie, and Deciphan.

10,000¢ Hacker Pyramid

Friday at 20:00 in Track 3

New for DEFCON 17 - The 10,000¢ Hacker Pyramid is a classic game show take off with the kind of pizzazz that only teams composed of average DEFCON Attendees and (in)famous DEFCON Celebrities could possibly bring to the stage. In a series of rounds, 8 teams will vie for the ultimate prize - 10,000 Canadian Pennies! There is no pre-qualification for this game, just be sure you're in the audience to be selected. Watch as Dick Clark's worst nightmares come true and a new DEFCON tradition is born. And don't feel bad for the losers - we've got prizes for them too—AWESOME prizes.

10,000¢ Hacker Pyramid Game Play

Beginning with eight teams total, playing four games. Each game will begin with 2 teams - one "celebrity" and one contestant each. At the beginning of their turn, a pair will choose one of 6 topics in the "pyramid". The attendee player is offered the choice of giving or receiving clues to/from the celebrity player. The teams are placed such that their members sit and face each other. The player giving the clues needs to see the board, while the other person faces away. In turn, each pair will be given 30 seconds to give clues describing each of 7 words/phrases per topic. Using any part of the word in the clue, results in an automatic pass (failure to score) on that word. The other player must attempt to guess the target word from the clues given. Players may also choose to pass if they are unable to complete the word. Points are awarded for each correctly guessed target word/phrase. Whichever team has the most points after 2 rounds moves on to the quarter final (two) games. From those four teams, playing against each other, 2 teams will remain in the finals.

Geo Challenge

See Schedule at defcon.org for times

What Is The Geo Challenge?

The urban environment of Las Vegas makes for some interesting geo caching. Add RFID embedded geo caches, puzzles & trivia that require tech knowledge, a live website that contains a progressive stream of puzzles & you have the Defcon Geo Challenge.

Objective

Teams of 2/3 will receive puzzles and clues via the contest website. Each puzzle will require a particular skill or knowledge for completion. Once completed a correct answer will reveal the next step in locating the Geo Cache coordinates. GPS coordinates will lead contestants to locations on the Vegas Strip where caches have been placed. Many caches will be disguised or in digital form requiring detailed searching and further decoding. Scoring will be based on multiple criteria, but mainly on the number of puzzles solved.

Equipment Required

Teams will be required to supply their own GPS device, Google Earth may suffice, but remember you will be looking for small objects that are made to blend into the surroundings, so accuracy is key. Teams are also required to have a portable computing device (PDA, Laptop, etc.) as answers can be submitted via the internet without returning to the contest area. Each team will be issued a RFID reader to assist in scanning of RFID embedded caches.

Prizes & Sponsors

The First and Second place teams will receive a nice package of prizes. Many thanks to all the sponsors who offered discounts on gear and donation of prizes. The response was great, especially for a first year event.

For More Info

Visit our booth or website.
http://www.defcongeochallenge.com
Syntax of DC210

Aside from the framework and techniques themselves, the Veritas Project hopes to present a number of current ongoing studies that uses "guerilla data mining". Ultimately, our goal is to provide as much information in how each study was done so other people can generate their own studies and share them through the project.

Hacking UFOlogy 102: The Implications of UFOs for Life, the Universe, and Everything

Richard Thieme, ThiemeWorks

Two years ago at Def Con 15, Richard presented Hacking UFOlogy. He supported his contention that (1) UFOs are real and (2) the data to support that statement is voluminous with numerous references and links which he encouraged others to explore in good old try-it-and-see hacker fashion. Who better than hackers to have open minds, a willingness to try new things, an ability to look deeply into systems, including systems of thought, to see how machinery can be made to do things its own inventors don't know.

Thieme builds on the foundation of that prior talk.

The core of this presentation is his belief that while economies and nation states come and go, the cosmos, like the Dude, abides, and the single most important event in the 21^st century will be the realization—not the speculation, not the movie, webisode, or tweet – but the full awareness that we are not alone in the universe ... and not the top of the food chain. We will know that as we know that space travel, dismissed by the Royal Astronomer as "utter bilge" in 1956, the year before Sputnik, is simply a fact.

Richard will draw on conversations with engineers, scientists, NASA personnel, aviation professionals and serious researchers over a period of thirty years.

Serious researchers? Like who?

Brad Sparks, for example. Brad discovered that the CIA concluded before the Robertson Panel in 1952 that UFO's were extraterrestrial. This was confirmed by the CIA director and deputy director of its Office of Scientific Intelligence. Brad also carried out a systematic investigation of the CIA's UFO activities, which included interviewing some 100 CIA Directors, Deputy Directors, Assistant Directors, and various intelligence officials of the CIA, NSA, DIA, Air Force and Naval Intelligence and other agencies, since 1975. He has reviewed 100,000's of pages of declassified CIA, NSA, AF, Army, Navy and other agency documents on UFO's and agency background histories in the course of his research and is reconstructing the full history of the U.S. Intelligence Community involvement with UFO's. Brad uncovered the important fact that the AF made a milestone policy decision on July 28,1952, to discount and/or reject anecdotal UFO reports and to henceforth stress instrumented and technical UFO detections and sightings, and he believes this is the watershed event in all of governmental history in UFO studies.

Brad is one. Michael Swords is another. Jerry Clark is another. There are more, they are rock solid, and their work is not trivial or frivolous.

These are formerly hidden members of a no-longer-invisible college who have been compelled by disinformation campaigns to color outside the lines of orthodox research, while that research nevertheless took place under cover of other activities. Thieme will illuminate why this is not a "conspiracy theory" but simply how things are done and have been done since 1945.

Fascinating documents will be provided. Entertaining stories will be told. Research will be documented. All will point toward a conclusion identical to the hypothesis: the single most important event in this century will be the realization that we are not alone in the universe. Human history must be remythologized. The system must be rewired.

Who better than hackers to think about these things?

Hacking, Biohacking, and the Future of Humanity

Richard Thieme, ThiemeWorks

I was asked in 2006 at AusCert in Australia, my second of three years of keynoting, where did I see hacking headed in the future? I described biohacking and noted that genetic engineering, neuroscience (both black and white R&D) and the availability of everything one needs for a few thousand bucks to hack the genome in a garage, all made hacking human attributes and identity the next level of the transformation of human possibility.

This talk illuminates how current and future developments in information systems, robotics, biotechnology, nanotechnology, and the colonization of the solar system through telerobotic and human exploration, all suggest ways human identity will be hacked and enhanced. The evolution of post-human identity is in our hands. This talk sounds like science fiction but isn't. It delivers profound insights into the next chapter of human civilization.

Invisible Access: Electronic Access Control, Audit Trails and "High Security"

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

This presentation will include a detailed review regarding the protection of high security facilities, including airports and aircraft, power transmission facilities, and data center rooms. The emphasis will be on liability and security issues that may result from an undue reliance on certain high security locking systems and the resulting Audit Logs that may not even exist. We will discuss a number of misconceptions and why these facilities may be at risk, even with some of the most sophisticated physical and electronic access control hardware and software.

Specific problems inherent in conventional locking hardware will be the primary focus, together with an analysis of high security mechanical locks and electronic access control systems produced by many of the Assa Abloy companies. These technologies include the Cliq, Logic, and NexGen among others. The representations of certain manufacturers will be analyzed, and potential vulnerabilities in these high-tech systems will be explored, together with the liability that may flow to users if these systems are circumvented.

Since the publication of OPEN IN THIRTY SECONDS , which details the compromise of Medeco high security locks (2008), intensive research has been on-going in the U.S. and Europe regarding the security of different electronic access control systems.

Metasploit Goes Web

Efrain Torres, Metasploit Team

This topic will present and discuss the new Metasploit plugin for web exploitation and assessment. WMAP is part of the Metasploit framework and it is build with a different approach compared to other open source alternatives and commercial scanners. WMAP is not build around any browser or spider for data capture and manipulation and as test modules are implemented as auxiliary modules they can interact with any other MSF components including the database, exploits and plugins. Forget about this being another scanner, think of it as new building blocks for massive pwnage that crosses protocol boundaries.

Good Vibrations: Hacking Motion Sickness on the Cheap

Tottenkoph consultant, crypto-fiend, hacker, and awesome chix0r

Motion sickness has been an issue since man learned how to travel by means other than by foot, with the earliest recorded cases dating back to ancient Greece.

Although the problem has existed for such a long time, there has been no documented case of a cure for all forms and severities of motion sickness and the most common way to relieve people of the symptoms that go along with motion sickness involve taking drugs. In this presentation, Tottenkoph will give an overview of what causes motion sickness as well as introduce a set of devices that will help lessen the severity of the symptoms that can be made easily.

MetaPhish

Valsmith, CEO, Attack Research
Colin Ames, Security Researcher
David Kerb, Security Researcher

Attackers have been increasingly using the web and client side attacks in order to steal information from victims. The remote exploit paradigm is shifting from the open port to the browser and email client. Penetration testers need to take these techniques into account in order to provide realistic tests.

In the past several years there have been numerous presentations on techniques for specific client side attacks and vulnerabilities. This talk will focus on building a phishing framework on top of Metasploit that pen testers can use to automate phishing and increase their overall capabilities. We will also cover some techniques for SpearPhishing on pen tests, second stage backdoors, and extensive communication over TOR.

Proxy Prank-o-Matic

Charlie Vedaa, Founder, PacketProtector.org
"Anonymous secondary speaker"

The Upside-Down-Ternet was just the beginning. What else can you do with a proxy server and a mischievous mind? We'll show you how to send your victims back in time (fun with archive.org), to the all-porn Internet (is there any other kind?), or to the Tourette-net (Cartman runs the Internets)! Via browser settings or port forwarding, using your Squid server or ours, you'll learn how to torment your friends in 20 fast-paced minutes.

USB Attacks: Fun with Plug & 0wn

Rafael Dominguez Vega, Security Researcher

How many times have you been handed a USB device and asked to copy a presentation or spreadsheet onto it? Often our biggest concern is around whether the device will be lost along with our company projections or takeover proposals. However, should we be more concerned about whether the device itself can be used to attack us and gain access to our system.

In the past USB security has often focused on the contents of the devices themselves. When considering the information that has been lost on unsecured devices it is quite understandable that this has received so much attention. However, in all this excitement have we lost perspective on where the real danger lies? If you want to know the answer to that question then you need to come along to the talk and find out.

The presentation will cover a wide range of security considerations for USB devices. However, it will specifically focus on the evolution of an attack that can be delivered through a malicious USB device. The talk will also include discussion about the methods that can be used to identify and exploit vulnerabilities in USB drivers and their advantages and disadvantages.

To highlight the reasons for conducting this research the presentation will also include the disclosure of a vulnerability affecting a USB driver in a common operating system that the audience will be very familiar with. It will also show how that can be exploited by simply plugging a malicious device into the system.

Hacking with GNURadio

Videoman

This presentation I will focus on the requirements for GnuRadio, cost, code, and radio technology basics. I will also present some of attacks that have been created using the GnuRadio, as well as my own research from a successful hack of a proprietary Multiple Address System (MAS) SCADA network, and a quick demo of the GnuRadio in action.

Videoman has 9+ years of experience doing computer security. He has worked for large enterprise financial institutions to secure their networks. Currently a computer security consultant, he enjoys working for NetSPI's clients to help them reduce their risks. In his spare time he and his wife run the local DefCon Group (DC612), and help to run the network at DefCon. He also likes to brew beer, and bike the many miles of pathways in Minnesota.

Cracking 400,000 Passwords, or How to Explain to Your Roommate why the Power Bill is a Little High…

Matt Weir, PhD Student, Florida State University
Professor Sudhir Aggarwal, Florida State University

Remember when phpbb.com was hacked in January and over 300,000 usernames and passwords were disclosed? Don't worry though, the hacker only tried to crack a third of them, (dealing with big password lists is a pain), and of those he/she only broke 24%. Of course the cracked password weren't very surprising. Yes, we already know people use "password123". What's interesting though is figuring out what the other 76% of the users were doing. In this talk I'll discuss some of my experiences cracking passwords, from dealing with large password lists, (89% of the phpbb.com list cracked so far), salted lists, (Web Hosting Talk), and individual passwords, (TrueCrypt is a pain). I'll also be releasing the tools and scripts I've developed along the way.

Hacking WITH the iPod Touch

Thomas Wilhelm, Sr. Network & Information Security Engineer; Adjunct Processor

There has been plenty of news about hacking into the iPod Touch, but what about using the iTouch as a hacking platform? This talk will discuss how to convert the iTouch into a PenTest device, describe available tools, and talk about potential uses for the iTouch as a social engineering tool to provide unauthorized access within a target network. We will also see real-world examples of the device in action against vulnerable systems.

Cross Site Scripting Anonymous Browser 2.0

Jeff Yestrumskas, Security Researcher
Matt Flick, Principal, FYRM Associates

Cross Site Scripting Anonymous Browser, Version 2.0 Earlier this year, the Cross-site Scripting Anonymous Browser ("XAB") was presented as a new perspective on how we could extend the functionality of browser technologies, form dynamic botnets for browsing, and create an unpronounceable acronym all at once. We continue the madness with the second incarnation of the XAB framework.

XAB hasn't really revolutionized attacks or defenses in its short lifespan, nor is it great at factoring primes. However, it has opened the minds of a few by demonstrating an interesting way to combine unlike ideas and creating a new animal all of it's own. Think of it as forced social networking, without ever really knowing whom you're talking to, or what they're saying.

We will provide a brief review of the technology, pour over the trials and tribulations of the enhancements and additions of the past 6 months, provide a live demonstration of the improvements and continue the conversation about the future of the framework.

Doppelganger: The Web's Evil Twin

Edward Zaborowski, Senior Security Engineer, Apptis

Users and administrators alike surf the web assuming that, for the most part, what they are looking at is what the website served to their browser; however, an attacker can deploy a malicious proxy, altering responses and requests, as well as potentially stealing sensitive data, all without a user being aware.

In this presentation I will discuss some of the attacks that a hacker can use when deploying a malicious proxy. Additionally, I will discuss Doppelganger, a tool that I've written to expedite some of the discussed techniques, its current capabilities, future additions, and more.

PLA Information Warfare Development Timeline and Nodal Analysis

Zulu Meet, Analyst, Verisign iDefense

The development timeline is consistent with the broad contours of China's current IW theory. It showed clearly the footprints of China's common war preparation patterns and People's war concept. For China, IW is a People's War, beyond simple "hacking," and is a long-term strategy that considered a necessary component for total war preparation. China has thus integrated IW units at multiple layers into the civilian and national emergency infrastructure. Also, ten years of practicing suggests that China has developed a mature understanding of IW and methodology, which it is able to quickly deploy and duplicate.

Criminal Charges are not pursued: Hacking PKI

Mike Zusman, Intrepidus Group

"From the night of Friday to Saturday at the 20 of December a new subscriber named Mike Zusman registered at the CA site. Subsequently he succeeded in overcoming the domain validation interface by validating for domains not under his control."—Critical Event Report

The last year has been a rough one for SSL PKI. Fraudulently provisioned certificates, MD5 collisions, SSL spoofing attacks, and most recently, attacks against EV SSL. The variety of these attacks shows us how big the attack surface of SSL really is. From crypto attacks to browser design flaws, attackers have choices when it comes to man-in-the-middling SSL protected web sites. This presentation covers one of these vectors: real attacks against CA web sites. While some folks look to CAs for guidance when it comes to conducting secure business on the Internet, the CAs themselves can fall victim to the same attacks consumers look to them for protection against. EV SSL is a step in the right direction, but with a heavy reliance on low-assurance domain validated SSL certificates, can we ever get SSL right?

Panel : Ask EFF: The Year in Digital Civil Liberties

Kurt Opsahl, Senior Staff Attorney, Electronic Frontier Foundation
Jennifer Granick, EFF Civil Liberties Director
Kevin Bankston, EFF Senior Staff Attorney
Fred von Lohmann, EFF Senior Staff Attorney
Marcia Hofmann, EFF Staff Attorney
Peter Eckersley, EFF Staff Technologist

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: Meet the Feds 2009

Jim Christy DC3
Mike Convertino Air Force
John Garris NASA
Barry Grundy Treasury
Bob Hopper NW3C
Mischel Kwon USCERT
Robert Lentz OSD/NII
Rich Marshall NSA
Stephane Turgeon RCMP
Shawn Henry FBI
Ken Privette USPS IG
Paul Sternal DCIS
Jamie Turner NCIS
Lin Wells NDU
Rod Beckstrom Ex-DHS
Jerry Dixon Ex-DHS
Andy Fried Ex-IRS
Greg Garcia Ex-DHS
Jon Idonisi Ex-Navy
Ray Kessenich Ex-NCIS/DCITA
Kevin Manson EX-FLETC
Keith Rhodes Ex-GAO

Did you ever wonder if the Feds were telling you're the truth when you asked a question? This year we're inviting you to "Meet the Feds and Ex-Feds" to answer your questions. The objective is to get you the answers to your questions without getting a public official fired! Our goal, probably not yours! Come ask your question and compare the answers you get.

With representatives from Defense Cyber Crime Center (DC3), FBI, IRS, NCIS, NASA, DHS USCERT, DoJ, NSA , National White Collar Crime Center (NWC3), NSA, US Postal IG, Office of the Secretary of Defense, National Defense University 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.

For years Defcon participants have played "Spot the Fed." For the 4th year, the feds will play "Spot the Lamer". Come out and nominate a Lamer and watch the feds burn' em.

night at the movies

Break Out Room

Each year I try to pick a couple movies for people looking for a break from con madness. This year I'm going to go with three movies, one a night, that I hope are new to most people.

Friday, 21:00 to 22:30
Gattaca (1997) Special Edition BluRay, 106 minutes
I've never actually seen this movie, but from what I have heard, the people who reccomend it, and the movie reviews I have read my hopes are very high. From johnbee-2:

> "Gattaca is a brilliant under-rated piece of cinema that the not-too-distant future will, in retrospect, see it as one of the more outstanding movies of the nineties. It is prolific, stylish, thought-provoking, and one of the few recent science fiction movies that totally foregoes special effects and does it well."

Saturday, 21:00 to 22:30
Stand Alone Complex Solid State Society (2006)
Everyone knows I enjoy the Ghost in the Shell manga and animie. This is the latest master work from Masamune Shirow, Kenji Kamiyama, and Studio I.G.

> "A.D. 2034. It has been two years since Motoko Kusanagi left Section 9. Togusa is now the new leader of the team, that has considerably increased its appointed personnel. The expanded new Section 9 confronts a rash of complicated incidents, and investigations reveal that an ultra-wizard hacker nicknamed the "Puppet Master" is behind the entire series of events."

DJ Delchi reccomends "Riders of the Storm" Dennis hopper and 5 insane people steal a B-29 bomber and convert it into an airborne pirate TV station..." S&M TV" jamming stations across the nation" As well as "The Quiet Earth" Oz film. An experiment to put a free energy grid around the planet results in everyone but 3 people disappearing from the planet. Classic scene when guy goes nuts.
I was tempted to play "Fragile Machine", an indie anime with almost no speaking that explores the eternal question of "Why am I here?" after a human computer interface experiment goes wrong and end up killing the human.. but a year later her brain gets copied to a android body and she continues on. I'll bring it along just in case.

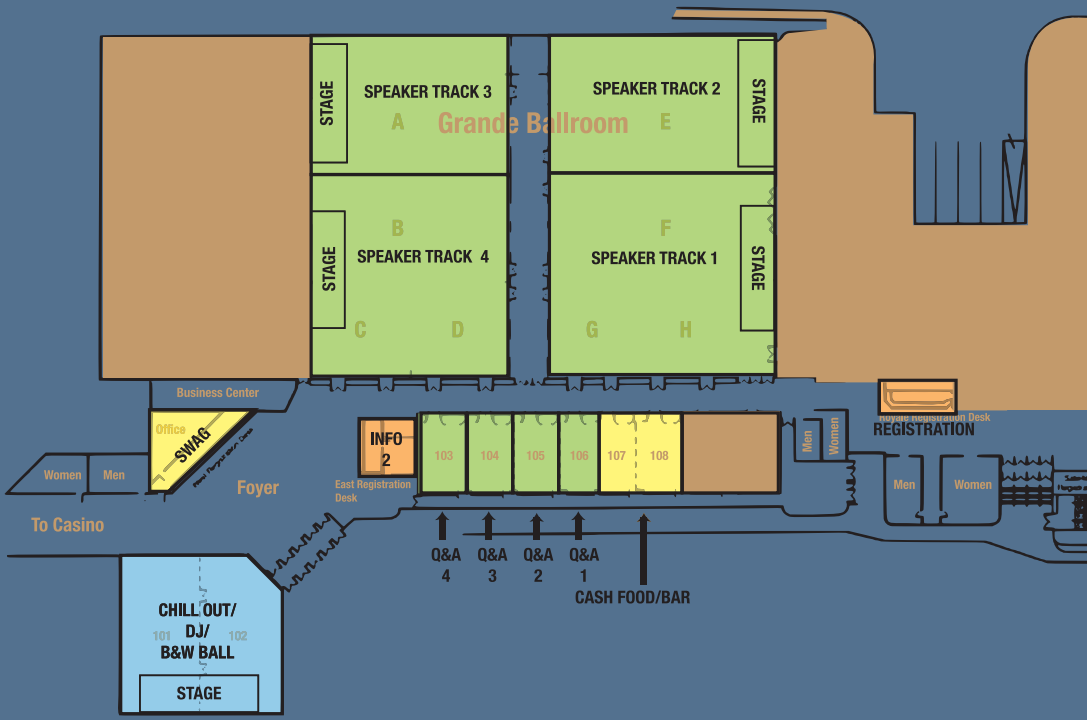
thursday

	Track 1	Track 2	Track 3	Track 4	Capri 103/104
13:00	**DEFCON 101** Panel	**Effective Information Security Career Planning** Lee Kushner & Mike Murray	**Hardware Black Magic - Building devices with FPGAs** Dr. Fouad Kiamilev	**Hacking with GNURadio** Videoman	**Pre-Con Introduction to Lock Picking** Alek Amrani
15:00				**Hacking the Apple TV and Where your Forensic Data Lives** Kevin Estis & Randy Robbins	
16:00	**Con Kung-Fu: Defending Yourself @ DEFCON** Rob "Padre" DeGulielmo	**DCFluX in: The Man with the Soldering Gun** Matt Krick "DCFluX"	**Defcon 1: a Personal Account** Dead Addict		**DC Network Session** Lockheed Until: 19:00
16:30	**So You Got Arrested in Vegas...** Jim Rennie				

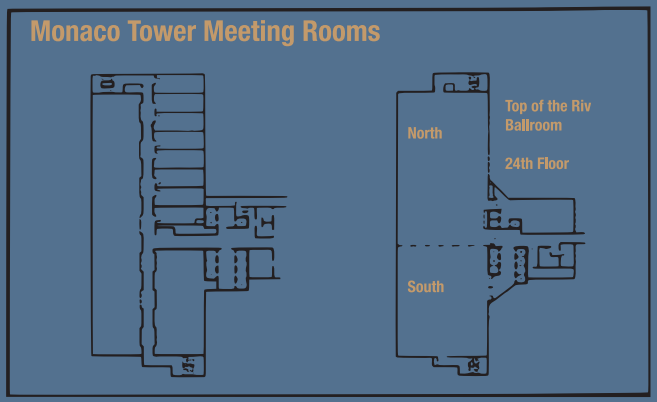
friday

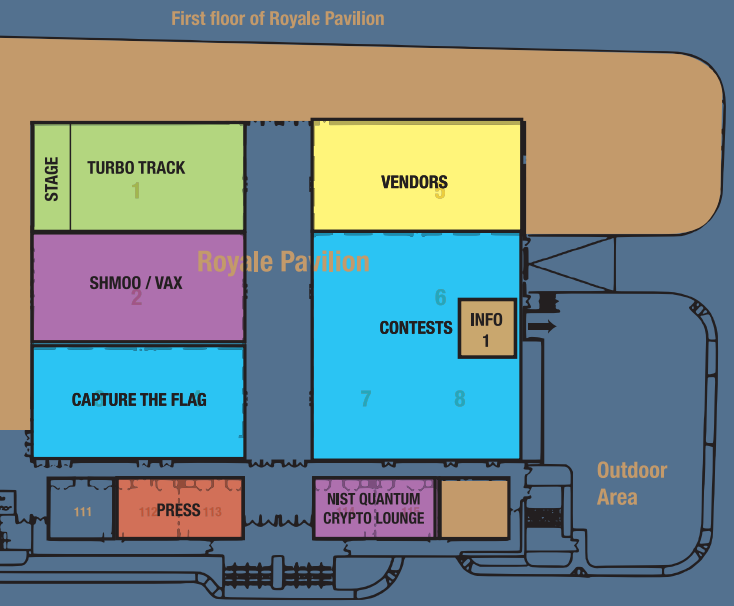
	Track 1	Track 2	Track 3	Track 4	Turbo/Breakout
10:00	**Welcome to Defcon 17 & the Making/Hacking the Badge** Joe Grand & The Dark Tangent	**Perspective of the DoD CSO** Robert Lentz	**Is your Iphone Pwned?** Kevin Mahaffey, John Hering and Anthony Lineberry	**Beckstrom's Law** Rod Beckstrom	**Catching DNS Tunnels with AI** Jhind
11:00	**Q & A with Bruce Schneier** Bruce Schneier	**Asymmetric Defense** Efstratios L. Gavas	**Jailbreaking and the Law of Reversing** Fred Von Lohmann and Jennifer Granick Civil Liberties Director, EFF	**TBD**	**Binary Obfuscation from the Top-Down** Sean Taylor "Frank2"
11:30		**Hacking the Wiimote and Wii fit to help the Disabled** Josh Marks and Rob Rehrig			
12:00	**More Tricks For Defeating SSL** Moxie Marlinspike	**TBA** Kenshoto	**0-day, gh0stnet and the Inside Story of the Adobe JBIG2 Vulnerability** Matt Richard and Steven Adair	**Death of Anonymous Travel** Sherri Davidoff	**Cross Site Scripting Anonymous Browser 2.0** Jeff Yestrumskas and Matt Flick
12:30					**Cloud Security in Map/Reduce** Jason Schlesinger
13:00	**The Year In Computer Crime Cases** Jennifer Granick	**Maximum CTF** Psifertex	**Hacking WITH the iPod Touch** Thomas Wilhelm		**Socially Owned in the Cloud** Digividual
13:30					**Deblaze** Jon Rose
14:00	**Making Fun of Your Malware** Michael Ligh & Matthew Richard	**Subverting the World Of Warcraft API** Christopher Mooney and James Luedke	**Advancing Video Application Attacks with Video Interception, Recording, and Replay** Jason Ostrom and Arjun Sambamoorthy	**Defcon Security Jam 2: The Fails Keep on Coming** David Mortman et al	**Attacking SMS.** Brandon Dixon
14:30					**Advanced MySQL Exploitation** Muhaimin Dzulfakar
15:00	**Reverse Engineering By Crayon** Danny Quist and Lorie M. Liebrock	**That Awesome Time I Was Sued For Two Billion Dollars** Jason Scott	**Computer and Internet Security Law: A Year in Review** Robert Clark		**Proxy Prank-o-Matic** Charlie Vedaa and Anonymous
15:30					**Session Donation** Alex Amrani
16:00	**Malware Freak Show** Nicholas J. Percoco and Jibran Ilyas	**Three Point Oh.** Johnny Long	**Why Tor is Slow, and What We're Doing About It** Roger Dingledine	**Ask EFF: The Year in Digital Civil Liberties** Panel	**Stealing Profits from Stock Market Spammers** Grant Jordan
16:30					
17:00	**Criminal Charges Are Not Pursued: Hacking PKI** Mike Zusman	**Fragging Game Servers** Bruce Potter and Logan Lodge	**BitTorrent Hacks** Michael Brooks and David Aslanian		**Automated Malware Similarity Analysis** Daniel Raygoza
17:30					**Injecting Electromagnetic Pulses into Digital Devices** Paul F. Renda
18:00	**Something about Network Security** Dan Kaminsky	**Locally Exploiting Wireless Sensors** Travis Goodspeed	**Attacking Tor at the Application Layer** Gregory Fleischer Until: 18:50	**Meet the Feds 2009** Panel	
18:30					**Hacking UFOlogy 102** Richard Thieme

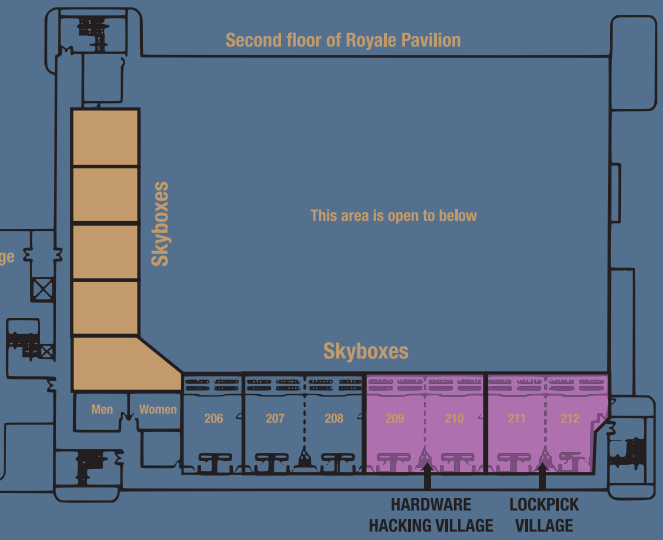
map • getting around



Monaco Tower Meeting Rooms







the network

WiFi Connections
802.11b/g - DefCon
802.11a - DefConA

Net access will be available in any of the convention areasall speaking rooms, CTF, Vendors, Contest area, and the side Capri rooms.

We have a whopping 20Mbps to the Internet–Everyone gets some!

Shouts-out to the NOC staff who keep this going every year: Lockheed, Heather, Videoman, efffn, Enki, Mac, Sparky, and KidKaos!

Got comments during or after the con? let us know–
noc@defconnetworking.org.

Check out post-con for stats and wrap-up at:
http://www.defconnetworking.org

saturday

	Track 1	Track 2	Track 3	Track 4	Turbo/Breakout
10:00	**"Smart" Parking Meter** Joe "Kingpin" Grand, Jake Appelbaum, and Chris Tarnovsky	**Breaking the "Unbreakable" Oracle with Metasploit** Chris Gates and Mario Ceballos	**Hacker vs. Disasters Large & Small** RenderMan and Michael "theprez98" Schearer	**Weaponizing the Web** Shawn Moyer and Nathan Hamiel	**Old Skool Brought Back** Phreakmonkey and Dr Kaos
11:00	**A Low Cost Spying Quadrotor for Global security Applications** Antoine Gademer and Corentin Chéron	**Using Guided Missiles in Drive-Bys** Egypt		**CSRF: Yeah, It Still Works** Mike "mckt" Bailey & Russ McRee	**Air Traffic Control** Righter Kunkel
11:30					
12:00	**RFID MythBusting** Chris Paget	**Metasploit goes Web** Efrain 'ET' Torres	**Personal Survival Preparedness** Steve Dunker and Kristie Dunker	**The Security Risks of Web 2.0** David Rook	**Packing and the Friendly Skies** Deviant Ollam
12:30					**Design of a Quantum True Random Number Generator** Sean Boyce
13:00	**Failure** Adam Savage	**Overflow Viewing Room for Adam Savage**	**Identifying, Exploring, and Predicting Threats in the Russian Hacker Community** Dr. Holt, Dr. Kilger, Dr. Strumsky, and Dr. Olga Smirnova	**Injectable Exploits** Kevin Johnson, Justin Searle and Frank DiMaggio	**Unfair Use** Dead Addict
13:30					
14:00	**The Projects of "Prototype This!"** Joe "Kingpin" Grand, Zoz	**MetaPhish** Valsmith, Colin Ames and David Kerb	**FOE: Feeding Controversial News to Censored Countries (Without Using Proxy Servers)** Sho Ho	**Abusing Firefox Addons** Roberto Suggi Liverani and Nick Freeman	**Smashing the Stack with Hydra** Pratap Prabhu and Yingbo Song
14:30					**Hardware Trojans** Stephen Janansky and Nick Waite
15:00	**Picking Electronic Locks Using TCP Sequence Prediction** Ricky Lawshae	**Metasploit Track** (continued)	**PLA Information Warfare Development Timeline and Nodal Analysis** Zulu Meet	**Hijacking Web 2.0 Sites with SSLstrip** Sam Bowne	**Making of the 2nd SQL Injection Worm** Sumit Siddharth
15:30					**Hacking the Smart Grid** Tony Flick
16:00	**Sniff Keystrokes With Lasers/Voltmeters** Andrea Barisani and Daniele Bianco			**Hadoop** Joey Calca and Ryan Anguiano	**Manipulation and Abuse of the Consumer Credit Reporting Agencies** Anonymous Speaker
16:30					**An Open JTAG Debugger** Travis Goodspeed
17:00	**Bluetooth, Smells Like Chicken Dominic Spill** Michael Ossmann and Mark Steward		**"I Am Walking Through a City Made of Glass and I Have a Bag Full of Rocks"** Jayson E. Street	**Clobbering the Cloud** Haroon Meer and Marco Slaviero	
17:30					**Doppelganger** Edward Zaborowski
18:00	**Router Exploitation** FX		**Preparing for Cyber War** Dmitri Alperovitch, Marcus Sachs, Phyllis Schneck and Ed Skoudis	**The Middler 2.0** Jay Beale and Justin Searle	**Sharepoint 2007 Knowledge Network Exposed** Digividual
18:30					**Runtime Kernel Patching on Mac OS X** Bosse Eriksson
19:00	**Closed**				**The Day of the Updates** Itzik Kotler and Tomer Bitton

sunday

	Track 1	Track 2	Track 3	Track 4	Turbo/Breakout
10:00	**Hello, My Name is /hostname/** Endgrain, Dan Kaminsky & Tiffany Rad	**Hacking, Biohacking, and the Future of Humanity** Richard Thieme	**Managed Code Rootkits** Erez Metula	**Down the Rabbit Hole** Iftach Ian Amit	**Advanced SQL Injection** Joseph McCray
11:00	**eXercise in Messaging and Presence Pwnage** Ava Latrope	**Hacking Sleep** Ne0nRa1n and Keith Biddulph	**Win at Reversing** Nick Harbour	**Invisible Access** Marc Weber Tobias, Matt Fiddler and Tobias Bluzmanis	**Hack like the Movie Stars** Cody Pollet and George Louthan
11:30					**Hack The Textbook** Jon R. Kibler and Mike Cooper
12:00	**Unmasking You** Joshua "Jabra" Abraham and Robert "RSnake" Hansen	**Good Vibrations: Hacking Motion Sickness on the Cheap** Tottenkoph	**Dradis Framework** etd	**Who Invented the Proximity Card?** Michael L. Davis	**Wi-Fish Finder** MD Sohail Ahmad & Prabhash Dhyani
12:30					**Attacks Against 2wire Residential Gateway Routers** Pedro "hkm" Joaquin
13:00	**Search And Seizure Explained** Tyler Pitchford	**Your Mind** James Arlen and Tiffany Rad	**Tactical Fingerprinting Using Metadata, Hidden Info and Lost Data** Chema Alonso and Jose Palazon "Palako"	**Lockpicking Forensics** Datagram	**Cracking the Poor and the Rich** Damian Finol
13:30					**AAPL** Da Beave and JFalcon
14:00	**Hackerspaces: The Legal Bases** RogueClown	**Slight of Mind** Mike Murray and Tyler Reguly	**Screen Scraper Tricks** Michael Schrenk	**RAID Recovery** Scott Moulton	**30k Feet Look at WiFi** Luiz "effffn" Eduardo
14:30					
15:00	**Robot Shark Laser! What Hackerspaces Do** Beth, Noid and Nick Farr	**Confidence Game Theater** cough	**Dangerous Minds** Mark Ryan Del Moral Talabis	**Protecting Against and Investigating Insider Threats** Antonio "Tony" Rucci	**USB Attacks** Rafael Dominguez Vega
15:30					
16:00	**Introduction to WiMAX Hacking** Goldy and Pierce	**Social Zombies** Tom Eston and Kevin Johnson	**Cracking 400,000 Passwords, or How to Explain to Your Roommate why the Power Bill is a Little High** Matt Weir and Sudhir Aggarwal	**The Psychology of Security Unusability** Peter Gutmann	**De Gustibus, or Hacking Your Tastebuds** Sandy Clark "Mouse"
16:30					
17:00	**Awards Ceremonies hosted by Dark Tangent**				

Shout outs! Word! Thank you! Props! Solid! Ack! In 'da haus! kthksbye!

Everything happened because these people got involved. Fluffy clouds & OMG Ponies to them all!

Ops and year round support: Charel, Nikita, Neil, Black Beetle, Zac, Jeff McNamara, CotMan, Converge.

The unstoppable DEF CON Network team: Lockheed, Heather, Videoman, efffn, Enki, Sparky, Mac, and KidKaos. As the mighty Netmaster 10BaseT says "I'm seeing all ones from the back o' the jack; I'm tellin' the telco they all smokin' crack. I can loop ya fuckin' link in a minute.Give me a console port...and I'm up in it."

The Skybox crew led by Grifter says thanks to kampf, and l3d. For wading through requests months before the con to select the best stuff for us to learn during the day, and the best parties to forget it all at that night.

Registration doesn't happen without TW, Tyler and Cstone.

Dispatch is handled by the ever smooth: Doolittle, Noise, Chuck, Rf, Josy, and Voltage Spike.

The many contests are overseen by Russ, who would like to send his shout out to Dark Tangent, Zac, Ping, Neil, hazmat72, Security Tribe, 303, pyr0, hackajar, dans, libero, phorkus, A, kampf, LosT, roamer, those groovy network goons, the terminator style security goons, Kingpin, zoz, siviak, deviant ollam, Vyrus, dc949, Moose, Shmoo, gmark, shrdlu, foofus, Winn, Logan Lodge, Chris Mooney, James Luedke, m@rs, vulc@n, sasha, nikita, mycurial, Syntax, Wall of Sheep, jackalope, and my super cool HHV volunteers (bombnav, ryan nelson, afterburn, ducksauz, voltagespike, scott hazel, mark smith, scott, and Fouad.). It takes a ton of effort, from a ton of individuals to pull off the contests and events. If you participate in anything at Defcon, thank that organizer! And finally, best wishes for hackajar and his family.

FAWCR would like to thank the following that make the Info Booth work:Dara, Flwrchld, Hazmat, Jenn, Lipgloss, Littlebruzer, Littleroo, mdmonk, Medic, Melloman, Sweep and Y3t1.

DEF CON Goons are handled by the ever prepared Noid. He thanks: Arclight, Che, Chosen1, CHS, Cjunky, Cyber, Cymike, Danozano, Dc0de, Eddy Current, Flea, Fox Captain, Freshman, Godminusone, Humperdink, John, Karenian, KevinE, KevinS, Krassi, Kruger, Lei, Londo, Lunaslide, MAXIMUS, Montell, noid, P33v3, Pappy, Pescador, Polish Dave, Priest, Queeg, Quiet, Rik, Skydog, Spahkle, Squeeky Penguin, vect0rx, Vidiot, Xinc, Ydobon, Angie, Lady Merlin, Candy, Evil, Xtacy, Al, Kallahar

Speaker Control who get everyone in the right place at the right time: Agent X, Quagmire Joe, Amish One, Nevada Raven, #2, Volty, Code24, Bushy, Xam, pwcrack, zendog, Dallas, Crash, a55mnky and Pardus.

For lighting, Décor and General Goodness at B & W Chill Out Area, and the Pool Décor Adam Ryan & Katya Rudneva, Sound Christian Manchester & Jon Cooper, Coordinators Travis Wyse & Trevor Wyse,

Visuals/Projections Kevin Whitesmith & Manuel Perez.

DJ and VJ coordinator and B & W Music Coordinator Scott Novich Party actions was aided greatly this year by GreatScott! and his team of DJ and lighting design ninjas: Miss DJ Jackalope, Undecided, Mumpi, Snow Crash,

Fillmatic, DJ Rene, njnTrubl, 8thNerve, Pepse, DJ Felix Kay, Digital Phreak, Corruptdata, Undecided, TRONA, The Scritch, Inconspicuous Villain, RECOGNIZE: The Goon Band, Phylo, E-Roc, Mitch Mitchem, SailorGloom, Krisz Klink, VJ

Q.Alba, DJ Reeves, Simo Sleevin, Simon Plexus, HoaX, DJ AMP, Pepse, DJ Felix Kay, 8thNerve.

The vendor staff: Chris, Wad, Wiseacre, Evil, AlxRogan.

Load in and out, QM stores: Uncle Ira, ETA, l3d, Major Malfunction, Alien, Dodger and RijilV.

DEF CON Schwag store: Q, SunSh1ne, Carine, Lucy, Mario & Veruus.

The return of the Original Goon and Wasz.

All of the speakers who took the time to develop presentations, test demos, and drop their info here first at DEF CON, and FAQ the newbies with content for the 1/2 day Thursday!

Also a special thanks to ComplexDrive.com for the great colocation services, the Riveria staff for getting better to work with every year: Conference Queen Teresa Madsen, Housing Diva Toni Goldsmith, Super Sales Stud Alan.

Joe Grand for all of his work wrangling the nightmare that is Chinese customs to try and get the badges he designed free in time for the con (Again!), DDTEK for taking on the huge responsibility of carrying the CTF torch and doing it with both humor and expertise.

—The Dark Tangent