
DEFCON
Bring your brains, leave the attitude.
13
www.defcon.org

TABLE OF CONTENTS

WELCOME TO DEFCON 13

Some say thirteen is an unlucky number, but I view it more as a transitional number. It can mean good or bad things. Plus there is no empirical evidence it is an inherently evil number, so fuck it.

This year team DEFCON has brought you a great line up of speakers, contests and events. Whether you are competing or just watching and learning I encourage you to get involved. Everyone makes a difference, and what you get out of DEF CON is up to you. An epiphany or a hangover, through Sunday night your mission is to enjoy yourself.

There are some exciting talks this year, and I'm telling you right now you won't make it them all. There are too many of them! The schedule is loosely built around different topics, and some of the well known speakers are up against each other. If you can hack your way into a room at the AP, youíre in luck. The speeches will be on hotel TV again this year.

This year there is an all new wireless network infrastructure. After saving money from the past few cons I spent a chunk of it on top of the line Aruba gear and plenty of access points. We'll need them in the years to come, and we may as well start playing with them now. Hacked up WAP11s are a thing of the past. To take advantage of all this new gear we doubled our bandwidth to 3MBit, and are doing some basic rate limiting and filtering to keep things rolling. There will be a captive portal page when you first associate to the network. From there you will get hourly updates of schedule changes, contest results, RSS feeds, and any anything else we feel like sharing. Phear the new WiFi a/b/g power!

If you have questions or need help, just look for a "Goon" in a red shirt. They are your friends, and are here to help. Different groups of staff at DEF CON have different color shirts depending on what they do, but the red shirts are there for the attendees.

When walking around the hotel with its new layout, don't forget to stop by the Info Booth where you can ask questions, learn about speaking changes and turn in or ask about lost items.

Too much happens for me to tell you, I don't even know myself until I get home and read about it all on-line. Speaking of which, after you have recovered take time to check out forum.defcon.org, www.defconpics.org and of course www.defcon.org. Share your pictures, post your stories, and download the presentations and music.

The Dark Tangent

P.S. Check out the closing ceremony to see who won what, and how they did it!

THE NETWORK @ DEFCON

SSID: DEFCON

Hope you brought your wireless card! This year we've gotten new equipment (Thanks DT!) and we're now offering 802.11 a, b, & g for breakfast, lunch, and dinner!

Net access is available in any of the public areas—the Parthenon complex, speaking rooms, tent, hotel lobby, bar area, and pool 1.

Rogue AP's? Never, not at DefCon! But just in case someone gets a crazy idea, check http://updates.defcon.org – we'll post the MAC addresses of the official DefCon AP's – anything else just isn't worth your time!

In addition to that, we've doubled our bandwidth this year; we've got a 3Mb connection to the evil Internet. Remember to share!

Big props out to the guys from Rant Radio – this is their second year in charge of the DefCon TV and the stuff you see on-screen (ticker updates, etc). Derek's taken charge of things, re-designed the flux capacitors this year, and provided a lot of cool back-end stuff. Together with AgentX providing the RSS feeds, we've done a lot this year to make sure you guys get the last-minute schedule changes as easily as possible!

Now…imagine being dropped into the middle of a desert and given 3 days to setup a solid network for a group of 5,000 hackers, secret agents, and fanny-pack carrying citizens. Plus keep it running! We just want to give shout-outs to the folks who make it happen, and spend several months planning this beast. Some are new to the network team, some have dedicated their adult lives to it: Lockheed (10 yrs), Heather (4yrs), Videoman (5 yrs), N8 (5 yrs), Connor (2yrs), Derek (2 yrs), Sqweak (2yrs), Skyroo (1 yrs), Major Malfunction (7 yrs)

Cheers!

The Dark Tangent exposes you to movies and video clips that he has found amusing over the past year. You may have seen some of these before, but now is your chance to grab a drink and chill out from the con and watch one with your friends. No friends? Well make some here. This year it is all Shirow, all of the time. Did I mention I like Shirow?

MOVIE ONE: Appleseed 2004 version

"If you can't kill yourself, build something to do it for you."

In years past we have brought you such goodies as Primer, Shaolin Soccer, and Equilibrium. This year I bring you a re-envisioned telling of Masamune Shirow's classic "Appleseed" done in CG 3-D rendering. Released in Japan in 2005, it is now available in English and is essentially a condensed version of the first Appleseed book. There were 4 books made, with Dark Horse releasing them in the States. I'm still waiting on book five, as is the rest of the fan base. I remember reading Appleseed comics in High School and dreaming of the future. The future isn't all that cool right now, but at least this movie is. 105 minutes.

MOVIE TWO: Ghost in the Shell 2: Innocence

GITS 2, not to be confused with GITS SAC (Stand Alone Complex) or GITS SAC 2nd GIG (The second season of GITS SAC) is the follow on to the first Ghost in the Shell. While it has nothing to do with the comic book series GITS, GITS 1.5 and GITS 2, it does provide excellent eye candy. While it is a bit slower than the first one, delving a bit too much into the metaphysical babble, the imagery and texture is very rich. The artwork at times is awesome, and I was left with the feeling that the animators and artists were showing off their skillz. Unfortunately this has not been released yet with an English audio track, so it will be subtitled.

If you watched Avalon with us last year, look for the same dog in GITS 2. It's modeled after the director's much beloved dog. 89 Minutes.

VIDEO CLIPS: Stand Alone Complex

"We are Soldiers, Stand or Die" About 70 Minutes.

If people are interested, three episodes from the first season of Stand Along Complex will be played. Don't worry; the audio track is in excellent English. I'll try and pick three action oriented episodes. While SAC ended a couple years ago, and SAC 2nd Gig ended last year, we in the States are just finishing up SAC on the Cartoon Network. Keep your eyes open for 2nd Gig next year.

A NIGHT AT THE MOVIES

TCP/IP DRINKING GAME

Like anything with 'Drinking Game' in its title, one of the primary objectives is to drink.

For this game you will need:

- 1 Master of Ceremonies / Moderator for the Game (Dr. Mudge)
- 1 Panel of self or industry proclaimed experts on TCP/IP internals
- (5 has proven itself to be a good number of panelists)
- 1 Rowdy audience of "Hackers" (easily found at DefCon or other Hacker conferences)
- 4-5 Cases of beer
- Some pretty sturdy livers...

The general premise of the game is simple. The audience proposes questions directed to the panel or directed to an individual on the panel. The questions should be something the audience member actually wants an answer to. After all, part of the Hacker-ethic is to take any opportunity that presents itself to LEARN (the MC is responsible for somewhat attempting to enforce this).

In the question posed by the audience member, for each term that is directly relevant (moderators call) to TCP/IP networking, a drink to the panel is accrued. If a picture is worth a thousand words, an example at this point is worth 6 drinks (in this case):

> Q: In a TCP packet, if the SYN, FIN, ACK, URG, and PUSH flags are all set what is this packet commonly referred to as?

In this case we count 'TCP packet' and each one of the flags listed explicitly as a drink. The panel or the panelist (moderators choice, though usually I'll loosen up the whole panel at the beginning of the game and then by making us all consume and then backing off to individuals as the game goes on) must consume 6 drinks for this question.

The answer to the question above would be a Christmas Tree Packet. If the panel or panelist does not know, or cannot come up with the answer much drinking ensues.

This is the first stage of the game. In later stages of the game the panel or panelist can negate drinks that are accrued in the question. If the panelist were to answer the previous question with something along the lines of:

> A: Having the SYN, FIN, ACK, URG, and PUSH flags set in a TCP packet is often referred to as a Christmas Tree Packet. However, it would be more appropriate to include the two reserved flags for explicit congestion notification in addition: ECN-Echo, and CWR (congestion window reduced).

The person answering the question has the ability to reduce the number of drinks already accrued in the asked question by using explicit TCP/IP and network related terminology in their response.

It starts going down-hill from here... And hopefully this time DT won't schedule the TCP/IP Drinking Game in the Morning again <grin>.

HACKER JEOPARDY XI

Hacker Jeopardy is back! For its eleventh year!

As usual, Hacker Jeopardy will be in the Outdoor Tent. The festivities begin at 22:00 on Friday, but people will be allowed in at 9:45PM.

Of course, we'll have the second night too, starting at the same time on Saturday.

If you're interested in submitting a team, go to the Contest Area in Athena and find the sign-up sheet. If you're interested in donating prizes to be given away during Hacker Jeopardy, you're able to drop them off at the NOC.

There will be plenty of prizes for the audience, good tech questions, plenty of booze, and a brand new Vinyl Vanna. Members of the winning team will take away a coveted DEFCON leather jacket.So don't miss out!

PGP KEYSIGNING WITH THE DARK TANGENT

Sign a PGP key today, starting with mine. The second annual PGP Keysigning.

I know that sounds selfish, but hey, you've got to be proactive about these things!

What I want to do is to revive the PGP party at DEFCON in a new streamlined fashion. With the advent of PGP key servers, such as pgpkeys.mit.edu, there is no need to do the floppy shuffle. All you need is the key ID and fingerprint of the person's key you want to sign. You search for that key on the key servers, and if the two match you are sure it is the right key for the right person.

PGP, and when I say PGP I also mean GPG, is a great security tool. But like any tool you have to use it properly to get the most out of it. In the case of PGP it comes down to a strong pass phrase, keeping your secret key file to yourself, and creating a web of trust.

To create that web of trust you need to sign other people's keys, and have yours signed as well. This has always been a pain in the ass because of the logistics of swapping floppies, etc.

To help facilitate this I have created a template for OfficeDepot micro-perf business cards. Use the template, and fill in your email address, key ID and fingerprint. Add a picture if you want. Then print a bunch of these out, and bring them to the con. Look for the PGP key exchange on the schedule, and show up to swap fingerprints with others. Heck, just hand them out all during con.

Download the template here:
http://www.defcon.org/dtangent/pgp-card-template.doc
http://www.defcon.org/dtangent/pgp-card-template.sxw

The goal is to increase the hacker web of trust with as little effort as possible. To do this you should take a few steps in advance:

1. Make sure your PGP key is valid and the one you want to use. Once people start signing it, it's a pain to discard it and start over.
2. Submit your key to keyserver.pgp.com. There are many others, but for ease of use we'll pick just one for now.
3. Print cards with your key ID and fingerprint. It would help to add your name or email address as well so people can remember who you are when it comes time for them to sign your key.

WHEN: JULY 30, 16:00 - 18:00
WHERE: ATHENA - AT THE INFO BOOTH

Once you have handed out your card and collected some from others it is time to process them after the show.

1. Search keyserver.pgp.com for the key id of the key you want to sign, and import it to your public key ring.
2. Sign that public key, and make sure to select Allow signature to be exported. This allows others to rely on your signature.
3. Send the signed key to the keyserver. On the graphical version of PGP for Windows or OS/X this is done using the send-to command. Highlight the newly signed key and send-to the server keyserver.pgp.com. It synchronizes the key you have with the key on the keyserver.
4. You are all done! The owner of the key can now check to see if you have signed their key.

Now it is time to check to see if anyone has signed your key.

1. Select your key and perform an update command. You will see your key that is found on the key servers.
2. Import it to your public key ring, and see if there are any new signatures on it.

Just to stay current it is a good idea every couple of months to update your own key, as well as the keys of others. On the commercial PGP version you just select all the keys on your keyring and perform an "update" command. It will go through all of your keys one at a time updating them.

If you have to revoke your key it is polite to submit the revocation to the key servers so others know not to use that key anymore.

OK, now that you have read this, go sign my damn key! I'll sign yours as well if I am sure you are who you say you are!
My PGP Key:
The Dark Tangent (RSA 2048)
<dtangent@defcon.org>
Key ID: 0x308D3094
PGP Fingerprint: D709 EAEB E09E DFC3
E47F 87AF 0EBE 0282 308D 3094

IMAGE COURTESY OF ZONEH

BEVERAGE COOLING CONTRAPTION CONTEST

In March of this year, the program MythBusters on the Discovery Channel featured an episode in which Jamie Hyneman & Adam Savage set about finding the fastest way to cool a six-pack. While they accomplished their goal by dousing cans of beer with the output of a CO2 fire extinguisher, their efforts at constructing actual devices to rapidly cool a beverage were less than successful. We'd wager that DefCon attendees could design and build beverage cooling contraptions that would blow the MythBusters away.

Think you've got what it takes to rapidly cool a cocktail? Then sign up for the Beverage Cooling Contraption Contest and put your hardware hacking skills to the test. There will be two categories of competition: cooling a beverage while it is still in its original, factory-sealed container & cooling a beverage which has been opened and poured out of its can and (ultimately) into a glass. The goal is to design a self-sufficient contraption which will cool a beverage to 38 degrees Fahrenheit as quickly and efficiently as possible without spending more than $100. For more information, check out http://deviating.net/bccc.

The contest will take place poolside on Saturday afternoon.

Check with the DefCon Info booth for details on the specific time and location.

CAPTURE THE FLAG

kenshoto is proud to present the WarGamez hacking contest. Our unique take on "Capture the Flag" is far more über than anything that has come before it.

Come behold the spectacle as you watch uber-nerds competing in knock-down, drag-out cyber-ninja warfare. This year, there will be far more real-time game data to keep spectators from getting bored.

Seven teams and eight individuals will compete to be the 1337357 of the 1337. In order to prove their f00, they will need to find and exploit vulnerabilities in custom software. This ain't no place for nessus—check your k1dd13 t00lz at the door. Teams will also have to defend a machine running all of these crappy services.

Those who can't reverse a binary, dream in asm, or stay in between the lines while coloring registers in the dark, will be excellent target practice for those who can.

Winners will be announced Sunday at DEFCON's closing ceremony.

Who Is Playing?

Last year's winner, Sk3wl0fR00t, is automatically qualified. Of the 120+ entrants into the qualifying round, only the following weren't totally lame:

Teams:

- Darwin's Bastards
- Digital Revelation
- Plan B
- Defconhackers
- Shellphish
- packet_loss

Individuals:

- individual
- tenos
- stejerean
- structure
- atlas
- cangaceiros
- plato

TCP/IP APPLIANCE CONTEST

Net-enabled devices have become more of a reality than fiction as computing power has increased and costs have decreased. Right now the industry is working on net enabling your home whether it's your television or your refrigerator. The purpose of this contest is to think outside of the box that the industry is thinking and create TCP/IP enabled devices that are fresh, new, cool, and literally way outside of the box.

There are two categories of devices in this contest.

The first category is TCP/IP embedded devices. These are stand alone devices which simply need to be plugged into a hub or switch. The device must host a TCP/IP aware service which someone can control and/or query a status from over a LAN or the internet and have it report back to the remote client that is controlling/querying it.

The second category is TCP/IP enabled peripherals. These are devices which must be connected to a host system such as a laptop or desktop computer which hosts the TCP/IP enabled service for the device. The host system must be able to communicate with the attached device in order to control it and/or query its status over a LAN or the internet and report back to the remote client which is controlling/querying it.

Devices in each category will be judged on originality, functionality, best value for actual cost and the coolness factor.

Three awards will be available. One for Best TCP/IP embedded device, Best TCP/IP enabled peripheral, and the Hax0r's Choice Award where your peers vote for what they think is the most uber elite device in the entire contest."

For More Information, visit the Contest and Info Booth in Athena or www.dc480.org

DEFCON BY PHONE

Defcon By Phone is an interactive voice response telephone-based schedule of the convention. It's more than just a replacement for your paper schedule; it will remind you when talks you're interested in seeing are about to happen, and it will let you know if they are rescheduled or cancelled. Use Defcon By Phone all weekend, then come and see Strom Carlson and Black Ratchet's talk on Asterisk on Sunday to find out more.

Call Defcon By Phone now at (800) 732-0442

DEFCON FORUMS MEETING

It's that time of year again. Since September 2001, the Defcon Forums have been providing a medium for Defcophiles to get together and build an online community. In fact, we get about 1,000 unique visitors per day, with nearly 10,000 users registered, 60,000 posts and 5,000 discussion threads! Why should Defcon only be three days a year? For some of us, Defcon is a lifestyle choice.

What: The Official Defcon Forum Meeting
When: Friday, July 28, 2005 from 2000 to 2200 (or later)
Where: Athena Room (Defcon Contest Area)
Why: A chance for forum users to get together and meet!

http://forums.defcon.org

DEFCON

ORGANIZED BY NULLTONE

WELCOME TO THE DEFCON 13 WARDRIVING CONTEST

This year's contest consists of 8 events. Two events will run simultaneously, one easy, one more difficult. Each team will have to choose to participate in the easy event, or the hard event. Easy events are worth 300 pts each. Hard Events are worth 1000. In some cases points are awarded only to the event winner. In others, points will be awarded (on a downward sliding scale) to first, second, and third places or partial points may be awarded.

Teams must choose which contest they will participate in at a given time (the easy one or the harder one). Teams may not split up and participate in both. In the event that teams submit results/participate in both games, they will not receive points for either. Teams may consist of 1 to 4 players.

Each contestant on each team must register on the DEF CON Forums. A limited number of registrations may be accepted on site at DEF CON 13. Each registered contestant must also check in with the WarDriving contest staff in the contest area at DEF CON 13. Each event will run for a maximum of three hours. Some of the easier games will run for less (in some cases only one hour).

One easy game and one hard game will run from 1100 - 1400 on Saturday and Sunday and the remaining games will run from 1700 - 2000 on Friday and Saturday.

Check-in: Once you arrive at DefCon, you will need to check in at the DefCon 13 WarDriving contest sign in area located in the DefCon Contest Area.

CONTEST DESCRIPTIONS

WarDrive (Easy: 200-300 points)
This year's WarDrive is simplicity itself. Teams have 2 hours to collect 1000 total access points. The first team to submit 1000 total access points will recieve 300 points. Each team that submits 1000 access points after that will receive 200 points. Results may be submitted to the contest staff via SFTP in the Contest area. Each team's combined results must be submitted in NetStumbler .NS1 format. Converters for Kismet to NetStumbler format will be made available through the Wardriving website.

Running Man (Easy: 300 points)
Object: Be the first to locate and identify the "Running Man."
Date/Time: Sunday 31 July, 11:00-12:00; Time limit of 1 hour

Fox and the Hound (Easy: 300 points to first team to locate the Fox. 200 points to second, 100 points to third)
Date/Time: Saturday, 30 July 11:00-14:00; Time limit of 3 hours
Object: Be the first team to locate the "Fox."

Tag (Hard: 1000 points to first, 750 to second, 500 to third, 100 to all others that successfully complete the task)
Date/Time: Saturday, 30 July 11:00-14:00
Object: The goal is to place a text file (yourname.txt) on the Desktop of a particular machine (C:\Program Files\Documents and Settings\All Users\Desktop). The first one that does wins. The text file must be in the format listed below and have your PGP public key so that we may confirm the winner.

The Last Crusade (Hard: 1000 points)
Date/Time: Sunday, 31 July 11:00-14:00
Object: Comprimise all 5 access points and get 1000 points.

King of The Hill (Hard: 1000 points)
Date/Time: Friday 29 July 17:00-20:00; The total time for this contest is 3 hours.
Object: Just like when you were a kid, the goal of "King of the Hill" is to get on top and stay on top.

LPCon/WD Contest Crossover (Hard: 1000 WD Contest points)
Date/Time: Saturday, 30 July 17:00-20:00;
Time limit: 3 hours
Object: Using DF skills track down an access point that is transmitting from inside a locked container. Pick the lock on the container and take physical possession of the Access Point.

The Lady and The Tramp (Easy: Up to 300 points on a sliding scale)
Date/Time: Saturday, 30 July 17:00-20:00
Object: Be the first one to compromise the "Tramp" and the "Lady" and then place your flag on the "Lady."

http://www.securitytribe.com/dc13wardrive/index.html

QUEERCON

Queercon got it's start last year when we realized there were a lot of queer hackers at Defcon, but no good queer parties. We decided to do something about it, and threw the most controversial Defcon party ever! The rainbow flag returns again this year in a new, bigger and better space. In true club style we'll have DJ CMOS (L.A.) spinning live, free glowsticks, and a cash bar. So come join the sexy queers Friday night starting at 2200 in Parthenon 2! All ages, all welcome.

Check out queercon.org for more info.

LPCON 3

THIRD ANNUAL LOCKPICKING CONTEST

The third annual DEFCON lock picking contest (LPCON3) will be held in the Athena room again this year. This is the opportunity for hobbyists and professionals to strut there stuff, and show just how good they really are. We've had a lot of fun this year, and with the help of some sponsors, hope this year is an even greater experience. To sign up for the contest, simply stop by the booth in the Athena. If you signed up online, don't forget to stop by and check in with us!

The contest runs from 1300-1600 Friday and Saturday afternoon. The event format welcomes participants as well as spectators. In fact, the pressure from performing in front of an audience can make even the fastest pick artist weak in the knees, so we hope to have people come by and share in the fun.

LPCON3 would like to thank lockpicking101.com, the Irvine Underground, and thenetworkadministrator.com for sponsoring the event this year. We've acquired a new group of locks for the contest this year which should be more robust, and more difficult thanks to our sponsors.

COFFEEWARS

Time to renew the time-honored hobby of teeth-grinding, hypertension and general caffeinated insanity. With Defcon comes The Defcon Coffee Wars!

Anyway, now's the time when you have an All-Inclusive Divine Excuse to unashamedly mingle with your own kind without having to shroud your activities under the shadow of the Evil Corporate Coffee Empire! Yes, now we caffeine fiends can gather without shame!

WHAT? You want a shot of espresso?! We got your shot right here, pal. This event ain't no freebie. If you want a cup, you gotta pony up. Coffee, that is. Whole bean. We're judging it all. The best, the strongest, the most caffeinated. You name it. ...but regular store-bought or corporate coffee trash will only earn a trashing.

You think you got what it takes? Then we'll take what you got! 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!

"If kids today chose coffee over methadone,
the world would be a far better and more productive place."
—AJ Rez

The Official DefCon
CoffeeWars

AMATEUR CTF KING OF THE HILL

1) Sign ups will be done at con (no exceptions)
2) You will get one point per minute for each service you hack on the victim
3) No hacking the scorekeeper
4) No spoofing as the victim system
5) No DoS/DDoS the scorekeeper nor the victim
6) We encoruage all contestants to make a small write up of the hacks they use, as these will be summarised and made avaliable as a "hand book" for later distribution.
7) no bitching (this contest is the first of many and a work in progress so bear with us Razz)

Visit the Info-Contest Booth in Athena for more details!

SPOT THE FED CONTEST

The ever popular paranoia builder. Who IS that person next to you?

Same Rules, Different year!

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 Priest's attention (or that of a Goon(tm) who can radio him) and claim out loud you think you have spotted a fed. 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 had 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. To qualify as a fed you should have some Law Enforcement powers (Badge / Gun) or be in the DoD in some role other than off duty soldier or Marine. What we are getting as is there are too many people with military ID angling for a shirt, so civilian contractors are not even considered!

To space things out over the course of the show we only try to spot about 8 feds a day or so. Because there are so many feds at DEF CON this year, the only feds that count are the kind that don't want to be identified.

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:
As usual 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. I've been doing this for a few years now, and I can honestly say I must have ten NSA mugs, two NSA cafeteria trays, and a hat. I'd be down for something more unusual this time. One year an INS agent gave me a quick reference card (with flow chart) for when it is legal to perform a body cavity search. Now that is cool. Be stealth about it if you don't want people to spot you. Agents from foreign governments are welcome to trade too. If I can't be found then Major Malfunction is my appointed Proxy.

WI-FI SHOOTOUT

At last year's contest, amateur engineering took a new turn as three teenage ham radio operators from Ohio established a new world's record (certified by the Guinness Book of World Records) for an unamplified wifi connection. Using two consumer-grade 32-milliwatt Orinoco Gold USB wifi adapters mounted on the feed points of two surplus 9-1/2 foot satellite dishes, the team known as P.A.D. achieved a verified connect distance of 55.1 miles (88.67 kilometers), without the use of external amplification. This year's contest is sure to once again shatter all preconceived notions as to how far a wifi signal can travel! As usual, this year's teams will be drawn from the pool of approximately 5000 Defcon attendees to see whose wifi reigns supreme! Spectacular prizes and fun are available to all who participate.

To enter, read all of the details at www.wifi-shootout.com, and then meet in the Athena contest room at noon on Friday or Saturday, July 29 and 30.

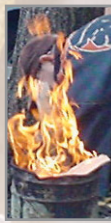
Sponsored by

WIRED

Trapeze

DEFCON Wifi Shootout

The Unofficial Defcon 13 Toxic BBQ will be held for its second year on Thursday, July 28th 18:00:00 until the event dies out. The event is held in the center of Sunset Park, between the parking lot and the pirate flag. Last year some 70 or so hackers met to grill and drink before the conference took off, this year we're doing the same.



Maps, information, and pictures available at www.toxicbbq.com

TOXIC BBQ

THE NIGHT BEFORE DEFCON

AS READ BY THORN TO HIGHWIZ AND STITCH

(With sincere apologies to the memory of Clement Clarke Moore)

'Twas the Night Before DefCon, in Steven Job's house,
A Support line rang and was answered by a louse.
"My new G4 is broke" ol' Roamer had said,
"What will you do? The fucking thing's dead."

"Just send it all back" the louse he replied.
"We'll fix it up quick, no matter how fried."
"There's just one little thing, that you really should know,
need all your passwords to make it all go."

"Are you fucking nuts?" Chris quickly returned,
"IF I give out my passwords, I'll surely be burned."
"You'll see all my p0rn, and my witty retorts,
"To all the DC guys, of whom I make sport."

"Like Alx, or HighWiz, or Medic or Noid"
and forty other people I have to avoid.
You'll grab all my JPEGs of titties and buns
And see all my code which makes it all run."

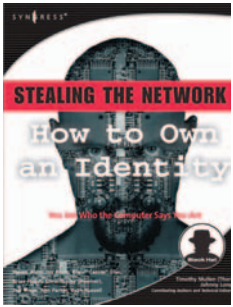
"Tough shit" said the louse, "We'll get what we need"
You signed our TOS, which you didn't read
We'll get all your p0rn, and your smart-assed replies,
As well as the IPs of those DC guys."

So the louse and his friends took Roamer's code,
When Chris saw the logs, he thought his head would explode.
But he crafted a plan, and created a site,
By which his cohorts would know of his plight.

This sad story is true, and the moral is plain,
If you piss Roamer off, you'll just end up in the Fucktard Hall of Fame .

_____

Thorn



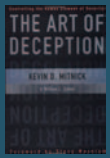
You Are Who the Computer Says You Are

The first two books in this series, Stealing the Network: How to Own the Box and Stealing the Network: How to Own a Continent, have become classics in the Hacker and Infosec communities because of their chillingly realistic depictions of criminal hacking techniques and strategies. But what happens when the tables turn, and the criminal hackers become the targets of both law enforcement and each other? What happens when they must evade detection by creating new identities and applying their skills to get out fast and vanish into thin air. In Stealing the Network: How to Own an Identity, the hacker crew you've grown to both love and hate find themselves on the run, fleeing from both authority and adversary. They must now use their prowess in a way they never expected—to survive...

BOOK SIGNING WITH THE CONTRIBUTORS ON FRIDAY @ 15:00

BOOKSIGNINGS

Richard Thieme
Fri, 1100



Kevin Mitnick
Fri, 1200

Johnny Long
Sat, 2000

Authors
Fri, 1900

Andrew Lockhart
Sat, 1200

Authors
Sat, 1500

Jay Beale
Sun, 1300

Authors
Sun, 1400

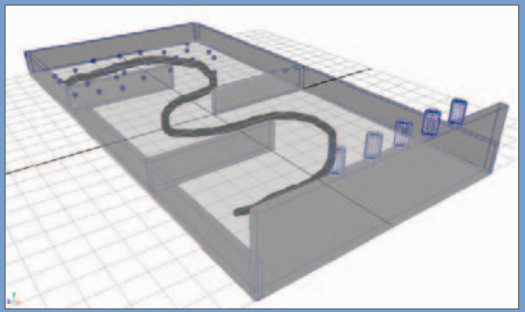
Books are available for purchase from BreakPoint Books.

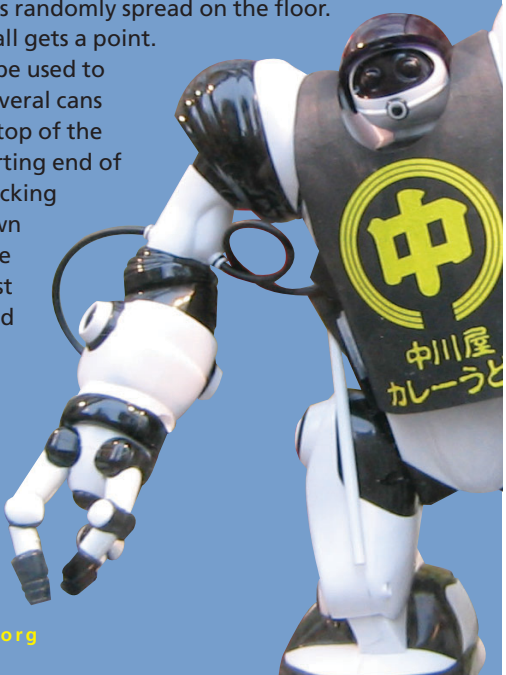
BOOKSIGNINGS ORGANIZED BY ROAMER

ROBOT WAREZ CONTEST

THE GOAL:

Each bot starts at one end of a rectangle, three walls are in the driving section which the bot must navigate to get to the other end. At the end are 25 ping pong balls randomly spread on the floor. Picking up a ball gets a point. The balls may be used to shoot down several cans placed on the top of the wall at the starting end of the arena, knocking those cans down are worth more points. The best score at the end of the timed match wins.





MORE INFO:

The remainder of the rules and details can be found here:
http://www.robotwarez.org/rules.html

Interested contestants should meet in the Contest Area (Athena) between 1045 - 1100, Friday morning for initial meet/greet and Q&A.

SPEAKERS

A New Hybrid Approach for Infrastructure Discovery, Monitoring and Control

Ofir Arkin, CTO and Co-Founder, Insightix

The first part of the talk presents the current available network discovery technologies, active network discovery and passive network discovery, and explains their strengths and weaknesses. The talk highlights technological barriers, which cannot be overcome, with open source and commercial applications using these technologies.

The second part of the talk presents a new hybrid approach for infrastructure discovery, monitoring and control. This agent-less approach provides with real-time, complete, granular and accurate information about an enterprise infrastructure. The underlying technology of the solution enables maintaining the information in real-time, and ensures the availability of accurate, complete and granular network context for other network and security applications.

During the talk new technological advancements in the fields of infrastructure discovery, monitoring and auditing will be presented.

Ofir Arkin is the CTO and Co-founder of Insightix, which pioneers the next generation of IT infrastructure discovery, monitoring and auditing systems for enterprise networks. Ofir holds 10 years of experience in data security research and management. Prior to co-founding Insightix, Ofir served as a CISO of a leading Israeli international telephone carrier. In addition, Ofir has consulted and worked for multinational companies in the financial, pharmaceutical and telecommunication sectors.

Ofir is an active member with the Honeynet project and is co-author of the team's book, "Know Your Enemy" published by Addison-Wesley. Ofir is also the founder of Sys-Security Group (http://www.sys-security.com), a computer security research group.

On the Current State of Remote Active OS Fingerprinting

Ofir Arkin, CTO and Co-Founder, Insightix

Active operating system fingerprinting is a technology, which uses stimulus (sends packets) in order to provoke a reaction from network elements. The implementations of active scanning will monitor the network for a response to be, or not, received from probed targeted network elements, and according to the type of response, and the conclusions following (part of an implementation's intelligence), knowledge will be gathered about the underlying operating system.

This talk examines the current state of remote active OS fingerprinting technology and tools: the different methods used today, the issues associated with them, the limitations, where the current technology is, what can and cannot be accomplished, and what should be done in the future.

The talk also highlights the accuracy aspects of several active operating system fingerprinting tools, analyzes them and compare between them.

During the talk a new version of Xprobe2, a remote active OS fingerprinting tool will be released.

Introducing the Bastille Hardening Assessment Tool

Jay Beale, Lead Architect, Bastille Linux

Bastille has been re-released as an assessment and hardening tool. With the help of the US Government's TSWG, we've added full hardening assessment capabilities, complete with scoring. This allows Bastille to measure and score an individual system's security settings against user-provided guidelines, possibly before allowing a system onto the network. Security or system administrators can use this to assess the relative state of a given system compared to Best Practices, to other systems in the organization, or to an organization-supplied minimum standards file. They can also use it to learn what hardening steps would be helpful for the given system. Bastille's new mode can even help in verifying compliance with new legislation, including Sarbanes Oxley, GLBA and HIPAA. It can also help in lowering insurance premiums—AIG, the largest provider of cybersecurity insurance, decreases premiums by 15% for organizations following best practices in proactive defense.

Open source tools have hardened systems in the past (Bastille, Titan, YASSP), while free or open source tools have measured security settings in the past (COPS, CIS Unix

Scoring Tool). No popular open source tool besides Bastille can do both, using the weaknesses found in an audit to harden systems. This functionality would normally be found only in a separate tool and thus warrants the re-release of Bastille.

We originally released Bastille Linux/Unix in 1999 as a host hardening tool, built to tighten security settings on a system, set stronger policies on that system and educate system administrators. Bastille has been extremely popular and has since been ported to seven Linux distributions, OS X and HP-UX. Support for FreeBSD and Solaris is underway. Bastille ships by default with Gentoo, Debian(apt-get) and HP-UX, the latter of which has made it part of the installer and contributes two developers to the project.

Jay Beale is a information security specialist, well known for his work on mitigation technology, specifically in the form of operating system and application hardening. He's written two of the most popular tools in this space: Bastille Linux, a lockdown tool that introduced a vital security-training component, and the Center for Internet Security's Unix Scoring Tool. Through Bastille and his work with the Center, Jay has provided leadership in the Linux system hardening space, participating in efforts to set, audit, and implement standards for Linux/Unix security within industry and government. He also focuses his energies on the OVAL project, where he works with government and industry to standardize and improve the field of vulnerability assessment. Jay is also a member of the Honeynet Project, working on tool development.

Jay makes his living as a security consultant with the firm Intelguardians, which he co-founded with industry leaders Ed Skoudis, Eric Cole, Mike Poor, Bob Hillery and Jim Alderson, where his work in penetration testing allows him to focus on attack as well as defense.

Mosquito - Secure Remote Code Execution Framework

Wes Brown, Senior Security Consultant
Scott Dunlop, Security Researcher

Mosquito is a lightweight framework to deploy and run code remotely and securely in the context of penetration tests. It makes a best effort to ensure that the communications are secure. Special care is taken to ensure that deployed code is not stored outside of process memory space, making it difficult for an eavesdropper to obtain the code. It protects the confidentiality and trade secrets of code that is deployed and run on the target, whether an exploit methodology, or a tool. The proof of concept deployable binary weights in at 120K. The framework makes use of Lua as the scripting language, and is freely available with a BSD license.

Wes Brown is a senior security consultant, security researcher, having started working in the field almost a decade ago. He specializes in penetration testing, and tools writing, but is greatly interested in conducting security research as well. He has written numerous in-house tools for Internet Security System's X-Force Consulting team, of whom he is a member of.

Scott Dunlop is a father, software developer, security researcher and short order cook, in that order; other public projects by Scott include Cloud Wiki, IPAF Packet Analysis Framework, and the Sickle Communication Language.

Development of An Undergraduate Security Program

Daniel Burroughs, University of Central Florida

At the University of Central Florida, an undergraduate program in security is currently being developed. This program will offer students a bachelor's degree through the College of Engineering. It is intended to be an interdisciplinary degree combining coursework from the School of Engineering and Computer Science, College of Health and Public Affairs, and the National Center for Forensic Studies.

The purpose of this talk is to present the program being developed and to receive feedback regarding what material and what areas such a program should cover. The department that it is being offered through (Engineering Technology) is an applied engineering department, taking a very hands-on approach to learning. As such it is necessary to develop our courses of study based on feedback from industry and the community.

Daniel Burroughs is currently an Assistant Professor in the College of Engineering at the University of Central Florida. His current research involves the development of the Florida Department of Law Enforcement Data Sharing Consortium and the development of a undergraduate security engineering program at UCF. His past work at the Institute for Security Technology Studies at Dartmouth College focused on using target tracking techniques to correlate data from multiple IDS and other sensors spread over large scale networks.

Auto-adapting Stealth Communication Channels

Daniel Burroughs, University of Central Florida

Intrusion detection systems and firewalls generally follow one of two methods of attack detection, signature or anomaly. Signature detection detects known attacks and anomaly detection covers unusual activity (with the hope that it will discover new attacks). Often what is detected by the IDS or firewall is not the original attack, but rather the communication that occurs afterwards. Known methods are easily picked up by signature detection, new methods are either picked up by anomaly detection or have a limited lifespan (signatures are created to detect them). That leads us to the dilemma of trying to create a covert communication scheme with no (easily) detectable pattern and one that does not cause statistical anomalies.

The key to solving this dilemma is to use a scheme that is not consistent in its appearance and adapts itself to match its current surroundings. The traffic on one network will very from that on another network. This means that what will look unusual or out of place on one network might not look so strange on another. By analyzing the conditions that exist on a network and then adapting the communication scheme to fit in with those conditions, a well camouflaged communication channel can be created.

This talk covers the concepts for such a communication system. It will cover the development and research being performed currently as well as providing a moderately technical discussion of the background concepts for such a system.

Be Your Own Telephone Company...With Asterisk

Strom Carlson & Black Ratchet

Since the invention of the step-by-step switching office by Almon B. Strowger in 1889, telephone switching technology has constantly become more efficient, more complex and easier to manage. Today, anyone with a computer, a telephone and some spare time can assemble a homebrew telephone switching system and become their own miniature telephone company with the aid of a program called Asterisk.

This presentation will give a brief overview of Asterisk, how to set it up, what it can do, and how to integrate it with your existing network. Furthermore, you will be introduced to a whole world of features and capabilities you didn't even know existed but which you will find yourself inexplicably compelled to set up and play with. Covered topics will include hardware, trunking, PSTN termination, integration with the Web and customization.

A Q&A session will follow the talk, accompanied by giveaways of selections from Strom's massive pile of vintage telephone equipment. If you can't make it to the talk itself, you will still be able to participate; a call-in Q&A queue will be provided for those watching the talk on TV in the hotel.

Strom Carlson is the organizer of DC213 and has been playing with telephones for years now; he has an intense interest in the structure and history of the telephone network and will start yammering away for hours about it if you're not careful. He collects all things related to telephony (including recordings), and although he is rapidly running out of space in which to store his many cubic meters of telephone equipment, he will eagerly and compulsively snap up anything made or published by Western Electric if given the chance. He encourages all phone phreaks and interested parties to play extensively with the phone network and learn everything they can; he also encourages you to listen to everything on www.phonetrips.com and to poke around www.stromcarlson.com

Black Ratchet is just another phone phreak from Boston. He enjoys computers, radios, and, of course, anything remotely related to the Public Switched Telephone network. He has been playing with telephones since he was eleven, and after a somewhat lengthy sabbatical in college, had a relapse and returned to his old ways in late 2003. He is the organizer and webmaster of Yet Another Payphone List at www.yapl.org and is an active member of the Digital Dawg Pound at www.binrev.com. He can be found at www.blackratchet.org, and on forums.binrev.com.

Analysis of Identity Creation Detection Schemes post-9/11

Cerebus

Have you wondered exactly how personal information is being used to help in the detection of Identity Creation in the post-9/11 world? Exactly how safe are social security numbers as a means to identity? How easy is it to create a valid SSN that will pass inspection by the Identity detection systems in place for business and government today? Or how you can recreate someone's SSN only knowing their date of birth and the last four digits of their SSN? This presentation will explain how current identity creation detection schemes work. You will leave understanding what

these schemes look for to flag someone as needing more investigation to establish that they are who they say they are. You will also learn about the history of the social security number, what the number means, and how it is used to establish identity.

Cerebus has worked for 10 years for one of the world's largest Marketing Database companies. He has designed Identity detection schemes for some of the top credit agencies in the US.

Routing in the Dark: Scalable Searches in Dark P2P Networks

Ian Clarke, Project Coordinator, FreenetProject Inc.
Oskar Sandberg, Department of Mathematical Sciences, Chalmers Technical University, Sweden

With peer to peer networks under fire by organizations using the legal system to attack participants, it seems that the only sustainable future is for dark, encrypted, networks where participants only talk to peers that they know and trust. Such networks, like WASTE, already exist to some extent, but they scale poorly and do not allow global communication.

This does not need to be the case, however. The "small world" observations, going back to Milgram's famous experiments in the sixties, show that social networks have all the right characteristics for being easy and efficient to navigate and search. It stands to reason that, under the right circumstances, so should a Darknet. We present algorithms for making routing possible in such networks, based on the real mathematics of how small worlds function. The goal is to build peer to peer networks that are difficult for outsiders to detect and infiltrate, making the job of those who wish to shut them down much harder.

Ian Clarke is the architect and coordinator of The Freenet Project, and the CEO of Cematics Ltd, a company he founded to realise commercial applications for the Freenet technology. Ian is the co-founder and formerly the CTO of Uprizer Inc., which was successful in raising $4 million in A-round venture capital from investors including Intel Capital. In October 2003, Ian was selected as one of the top 100 innovators under the age of 35 by the Massachusetts Institute of Technology's Technology Review magazine. Ian holds a degree in Artificial Intelligence and Computer Science from Edinburgh University, Scotland. He has also worked as a consultant for a number of companies including 3Com, and Logica UK's Space Division.

Oskar Sandberg is a post graduate student at the Chalmers Technical University in Gothenburg, Sweden. He is working on a PhD about the mathematics of complex networks, especially with regard to the small world phenomenon. Besides this he has an active interest in distributed computer networks and network security, and has been an active contributor to The Freenet Project since 1999.

Countering Denial of Information Attacks

Greg Conti, United States Military Academy, West Point, New York

We are besieged with information every day, our inboxes overflow with spam and our search queries return a great deal of irrelevant information. In most cases there is no malicious intent, just simply too much information. However, if we consider active malicious entities, the picture darkens. Denial of information (DoI) attacks assail the human through their computer system and manifest themselves as attacks that target the human's perceptual, cognitive and motor capabilities. By exploiting these capabilities, attackers reduce the ability of humans to acquire and act upon desired information. Even if a traditional denial of service attack against a machine is not possible, the human utilizing the machine may still succumb to a DoI attack. Typically much more subtle (and potentially much more dangerous), DoI attacks can actively alter the decision making of humans, potentially without their knowledge. This talk explores denial of information attacks and countermeasures and uses network visualization scenarios to illustrate the problem.

Greg Conti is an Assistant Professor of Computer Science at the United States Military Academy. He holds a Masters Degree in Computer Science from Johns Hopkins University and a Bachelor of Science in Computer Science from the United States Military Academy. His areas of expertise include network security, information visualization and information warfare. Greg has worked at a variety of military intelligence assignments specializing in Signals Intelligence. Currently he is on a Department of Defense Fellowship and is working on his PhD in Computer Science at Georgia Tech. His work can be found at www.cc.gatech.edu/~conti and www.rumint.org.

Sketchtools: Prototyping Physical Interfaces

Matt Cottam, Creative Director, Tellart; Faculty, Industrial Design, Rhode Island School of Design

Industrial designers working in traditional media have the luxury of sketching, playing, and experimenting with their materials before constructing a finished product. Designers working with electronics and computers are relatively impoverished. To "sketch" with electronics or computers would typically require extensive training in engineering and ready access to inexpensive parts—requirements that most designers can't easily meet. This deficiency—this inability to work closely with materials before building with them—hampers designers' efforts to make products sensitive to human use. This paper describes an attempt to address this problem in a human-computer interaction (HCI) design studio at a major design school. The course itself was an exercise in design: it worked within severe constraints to address a human need. We describe our attempt to shape the course to meet students' most pressing needs; our students' attempts to work within the constraints of the course; and the outcomes of the course for students and faculty. The paper suggests that the course offers one way to experiment with HCI concepts, produce innovative solutions to design problems, and—crucially—humanize new technologies and the design process."

Matt Cottam has a Bachelor of Fine Arts and Bachelor of Industrial Design degrees from Rhode Island School of Design (RISD). Matt's thesis work at RISD was to conduct human-factors research for the Habitability Design Division of NASA. Since 1998 Matt has been the core instructor of the Structured Multimedia Module of the International Certificate Program in New Media at the Fraunhofer Center for Research in Computer Graphics. Since 1999 he has been a member of the faculty at RISD; he teaches critical human-centered design and human-computer interaction design for the departments of Industrial Design, Graphic Design, Photography, and The Digital Media Graduate Program. Matt cofounded Tellart and specializes in human-computer interface design technology, methodology, and pedagogy.

The Information Security Industry: $3 Billion of Snake Oil

David Cowan, General Partner, Bessemer Ventures

A raging fear of The Computer Evildoers has driven enterprises to the safety of the herd, buying whatever elixirs the big vendors peddle. Security consumers waste billions of dollars on ineffective (but well integrated!) solutions. However, as technology users grow more sophisticated about security threats (often learning the hard way), opportunities will surface for innovative startups to deliver effective IT survival mechanisms. This talk will review the industry's blunders, and sources of opportunity.

David joined Bessemer Venture Partners in 1992. David has since made 43 early-stage investments for Bessemer, including 19 that have gone public, and 16 that have been acquired by public companies. David initially focused on communications technology companies like Ciena, P-Com, and PSI-Net, and then internet services such as Keynote, Flycast, Hotjobs and Blue Nile. In 1995 he cofounded Verisign as a Bessemer-funded spinout of RSA, serving as VeriSign's initial Chairman and CFO. His other data security investments have included Counterpane, Cyota, Determina, eEye, Elemental Security, Finjan, ON Technology (acquired by Symantec), Postini, Qualys, Tripwire, Tumbleweed, Valicert and Worldtalk (both of which Tumbleweed acquired). David also teaches computer science at the Keys Middle School in Palo Alto. He received both his B.A. in math and computer science and his M.B.A. degrees from Harvard University.

CISO Q&A with Dark Tangent

Scott Blake, Liberty Mutual
Pamela Fusco, Merck
Ken Pfiel, Capital IQ
Justin Somaini, Verisign
Andre Gold, Continental Airlines
David Mortman, Seibel Systems

The Dark Tangent, founder of DEFCON, invites Chief Information Security Officers from global corporations to join him on stage for a unique set of questions and answers. What do CISOs think of David Litchfield, Dan Kaminsky, Joe Grand, Metasploit, Black Hat, and DEFCON? How many years before deperimeterization is a

reality? Is security research more helpful or harmful to the economy? What privacy practices do CISOs personally use? These questions and others from the audience will be fielded by this panel of security visionaries.

Scott Blake is CISO for Liberty Mutual Insurance Group and is responsible for information security strategy and policy. Prior to joining Liberty, Scott was VP of Information Security for BindView Corporation where he founded the RAZOR security research team and directed security technology, market, and public affairs strategy. Scott has delivered many lectures on all aspects of information security and is frequently sought by the press for expert commentary.

Pamela Fusco is an Executive Global Information Security Professional, for Merck & CO., Inc. She has accumulated over 19 years of substantial experience within the Security Industry. Her extensive background and expertise expand globally encompassing all facets of security inclusive of logical, physical, personal, facilities, systems, networks, wireless, and forensic investigations. Presently she leads a talented team of Compliance, Systems and Information Security Engineers operating a world-wide 24X7X365 SIRT (security incident response team).

Ken Pfeil is CSO at Capital IQ, a web-based information service company headquartered in New York City. His experience spans over two decades with companies such as Microsoft, Dell, Avaya, Identix, and Merrill Lynch. Ken is coauthor of the books "Hack Proofing Your Network - 2nd Edition" and "Stealing the Network: How to Own the Box," and a contributing author of "Security Planning and Disaster Recovery" and "Network Security–The Complete Reference."

Justin Somaini is Director of Information Security at VeriSign Inc. where he is responsible for managing all aspects of network and information security for VeriSign. With over 10 years of Information Security and Corporate Audit experience, Justin has leveraged his knowledge of audit and large organizations to remediate global infrastructure problems and create a full risk identification and remediation Information Security group.

David Mortman, CISO for Siebel Systems, Inc., and his team are responsible for Siebel Systems' worldwide IT security infrastructure, both internal and external. He also works closely with Siebel's product groups and the company's physical security team. Previously, Mr. Mortman was Manager of IT Security at Network Associates, where, in addition to managing data security, he deployed and tested all of NAI's security products before they were released to customers. A CISSP, member of USENIX/SAGE and ISSA, and speaker at RSA 2002 and 2005 security conferences, Mr. Mortman has also been a panelist at InfoSecurity 2003 and Black Hat 2004.

Whiz Kids or Juvenile Delinquents: A Sociological Perspective The Construction of Hacker Identity

Amanda Dean

The paper I will be presenting serves as a rudimentary literature review on how hackers may be constructed as either deviants or non-deviants in society. This presentation begins by placing hackers within the framework of sociological literature on deviance. I talk about how deviance has historically been a social construction, with the more powerful members of society defining what it is to be deviant, and those with less power are frequently applied the label. I apply sociological definitions of deviants to hackers, and am able to refute these claims in many cases.

I am a doctoral student in the sociology department at the University of Nevada, Las Vegas. The vast majority of my friends are "techies," and as a social scientist, I'm a bit of an outcast. I mitigate some of that by focusing my research attention on the effects of technology on and within society. While getting my master's degree in Criminal Justice at Grand Valley State University, I began to look at some of the laws protecting information and technology, and their social consequences. For my dissertation, I'd like to turn my attention specifically on hackers, hactivism, and global social movements. In my spare time I'm a big time gaming geek which I balance with my addiction to drag racing and canyon carving on my sport bike.

Introduction to Lockpicking and Physical Security

Deviant Ollam

Physical security isn't just a concern of the IT world. Besides securing server rooms, locks of all sizes and styles are scattered throughout our lives. However, much of the general public is unaware of the insecurities present in many lock designs. Through discussion and direct example, Deviant Ollam will address the strengths and weaknesses of standard pin tumbler locks, combination locks, warded locks, wafer locks, and more. Discussion of effective tools, advanced techniques, master key

theory, and lesser-known picking techniques will also be covered. This talk is aimed at lockpick novices who are interested in better security and learning lockpicking skills. While always the first to admit that he's no Barry Wels, Deviant hopes to have a good time with this lockpick talk and looks forward to hand-on audience participation. Many styles of practice locks and picks will be made available.

While paying the bills as a network engineer, Deviant Ollam's first and strongest love has always been teaching. Employed periodically at schools in the greater Philadelphia area, he is presently a student at the New Jersey Institute of Technology in the hopes of tacking some actual letters to his name and doing the professor gig full time. A fanatical supporter of First Amendment rights who believes that the best way to increase security is to publicly disclose vulnerabilities, Deviant has given lockpick demonstrations at other con events and various schools.

The Hacker's Guide to Search and Arrest

Steve Dunker, Esq

Have you ever been pulled over by the Cops? Do you worry about your home being searched by the Feds? The Hacker's Guide to Search and Arrest is presented in a down and dirty fast pace. You won't hear a single boring case citation here. Instead you get information you can use in every day life, presented in a way that won't make your eyes gaze over. Learn when the Government can legally perform searches or make arrests. Find out what you can do if you are a victim of an illegal search or seizure.

Steve Dunker is a Professor of Criminal Justice at Northeastern State University. He is a former Major Case Squad Detective who worked as a planner and supervisor of an anti-crime and decoy unit. He is a licensed attorney in the State of Missouri.

The Power to Map: How Cyberspace Is Imagined Through Cartography

Kristofer Erickson, The University of Washington Department of Geography

An ongoing project for scholars in Geography has been to explore how power and cartography are mutually implicated. Geographers have traditionally been concerned with making maps of the earth, but until recently we have seldom reflected on how particular forms of knowledge and power are privileged in the production of maps, and how those maps themselves produce particular geographic imaginations. As new virtual spaces are opened up through communication technologies such as the Internet, maps remain one of the important ways that these spaces are articulated to the public. However, when creating these new maps of cyberspace, it is necessary to remain aware of the political meaning contained in these representations. Maps of the internet that depict it as a disembodied, decentralized and unregulated space may in fact promote particular interests such as capitalism and national security, while suppressing others. The aim of this presentation is to open up a dialogue where we can collectively critique existing maps of cyberspace and imagine alternatives that may be more sensitive to a competing range of interests, including those of the hacker community.

Kristofer Erickson is currently completing his PhD in Geography at the University of Washington in Seattle, where he teaches an undergraduate seminar on Law and Cyberspace. He is motivated by a desire to bridge the gap between academic scholarship and politics, which is one of the reasons he is thrilled to be able to present at Defcon. Recent notable accomplishments include attending the September Project, a nationwide effort to promote community discussion of democracy and freedom in local public libraries, legitimately playing a round of Final Fight on the jumbotron screen during an undergraduate college class, and standing up for the blogosphere in a roomful of old-guard Marxist academics in Denver Colorado.

Hacking Nmap

Fyodor

While many security practitioners use Nmap, few understand its full power. Nmap deserves part of the blame for being too helpful. A simple command such as "nmap scanme.insecure.org" leaves Nmap to choose the scan type, timing details, target ports, output format, source ports and addresses, and more. You can even specify -iR (random input) and let Nmap choose the targets! Hiding all of these details makes Nmap easy to use, but also easy to grow complacent with. Many people never explore the literally hundreds of available options and scan techniques for more powerful scanning.

In this presentation, Nmap author Fyodor details advanced Nmap usage—from clever hacks for teaching Nmap new tricks, to new and undocumented features for bypassing firewalls, optimizing scan performance, defeating intrusion detection systems, and more.

Fyodor authored the popular Nmap Security Scanner, which was named security tool of the year by Linux Journal, Info World, and the Codetalker Digest. It was also featured in the hit movie "Matrix Reloaded" as well as by the BBC, CNet, Wired, Slashdot, Securityfocus, and others. He also maintains the Insecure.Org and Seclists.Org security resource sites and has authored seminal papers detailing techniques for stealth port scanning, remote operating system detection via TCP/IP stack fingerprinting, version detection, and the IPID Idle Scan. He is a member of the Honeynet project and a co-author of the books "Know Your Enemy: Honeynets" and "Stealing the Network: How to Own a Continent".

A Safecracking Double Feature: Dial 'B' For BackDialing and Spike the Wonder Safe

Leonard Gallion

This presentation will introduce two powerful, non-destructive safe opening techniques. The first "Dial B For BackDialing," will trace the history of backdialing all the way from Richard Feynman working on the atomic bomb (and opening safes) in the 1940's, to today. This presentation will show how mechanical safes have changed since Feynman's time, but how most are still vulnerable to both his method and the simpler Nascar(tm) technique. The next part of the presentation, "Spike the Wonder Safe" will demonstrate how to defeat the two locking mechanisms of a popular office safe using just an ink pen and a battery, all in under two minutes.

Leonard Gallion, is the Vice President of Information Services for a Dallas Texas company and has over 20 years of experience in the I.T. and Security fields. Primarily focusing on the non-destructive (stealthy) compromise of physical security, he has publicly presented on such topics as lockpicking, safecracking and high security lock bypass. In addition, he published an article in the Summer 2004 issue of 2600 magazine on his hobby, creating "Impromptu Lock Picks" from common office supplies.

Hacking in a Foreign Language: A Network Security Guide to Russia (and Beyond)

Kenneth Geers

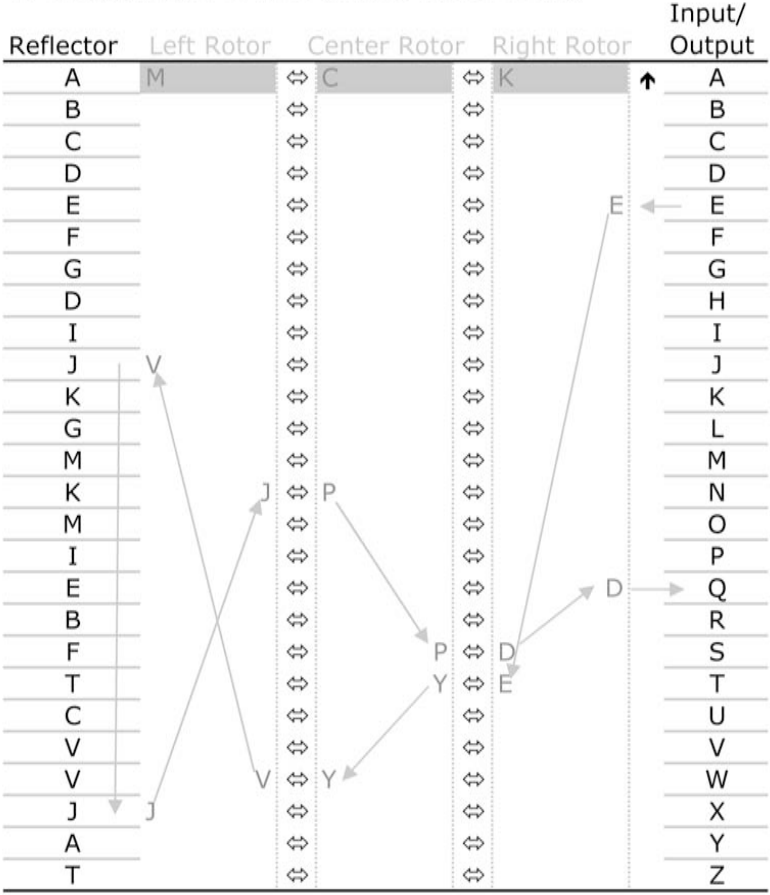
A brief introduction to Russia will be followed by 1,000 traceroutes over the frozen tundra described in detail, along with an explanation of the relationship between cyber and terrestrial geography. Information will be provided on Russian hacker groups and law enforcement personnel, as well as a personal interview with the top Russian cyber cop, conducted in Russian and translated for this briefing.

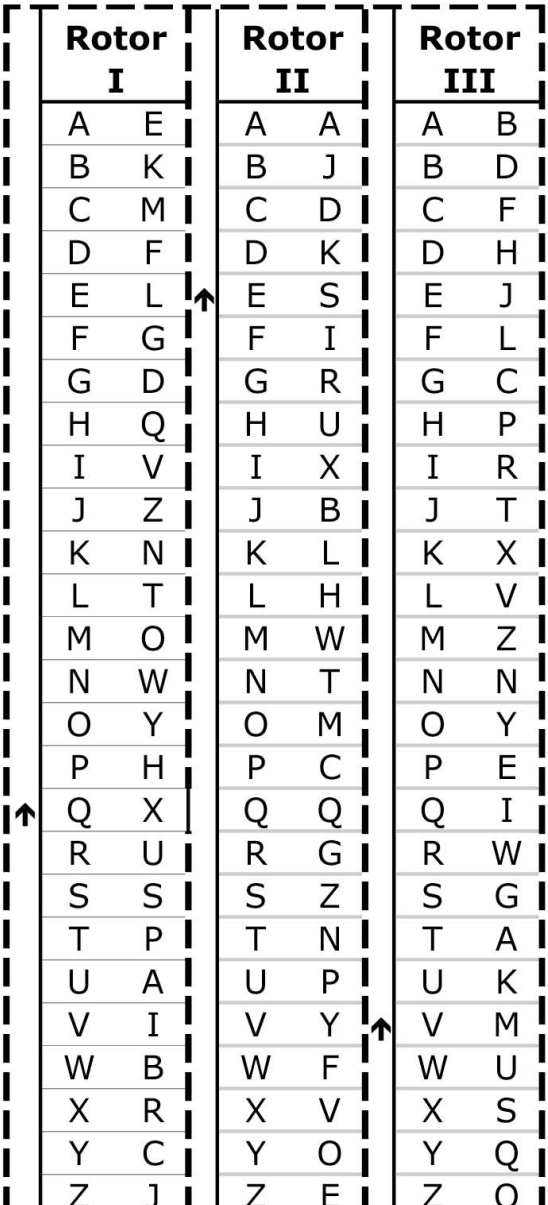
You will receive a short primer on the Russian language, to include network security terminology, software translation tools, and cross-cultural social engineering faux-pas (this method will apply to cracking other foreign languages as well).

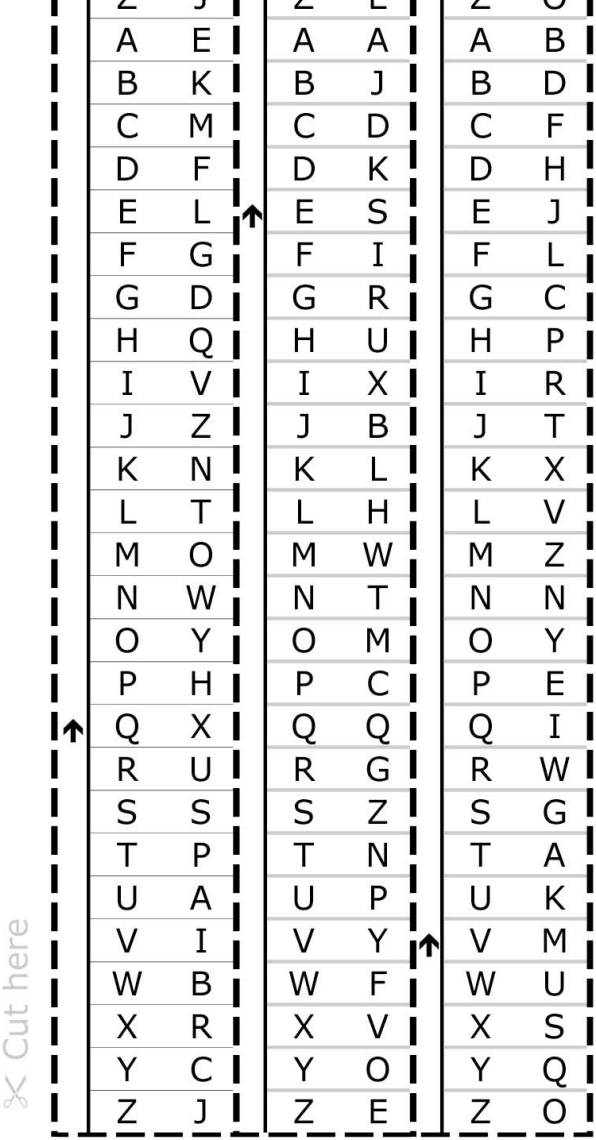
Hacking in a Foreign Language details a four-step plan for crossing international frontiers in cyberspace. First, you must learn something about the Tribe: in this case, the chess players and the cosmonauts. Second, you must study their cyber Terrain. We will examine the open source information and then try to create our own network map using traceroutes. Third, we will look at the Techniques that the adversary employs. And fourth, we will conquer Translation. The goal is to level the playing field for those who do not speak a foreign language. This briefing paves the way for amateur and professional hackers to move beyond their lonely linguistic and cultural orbit in order to do battle on far-away Internet terrain.

Kenneth Geers (M.A., University of Washington, 1997) is an accomplished computer security expert and Russian linguist. His career includes many years working as a translator, programmer, website developer and analyst. The oddest job he has had was working on the John F. Kennedy Assassination Review Board (don't ask). He also waited tables in Luxembourg, harvested flowers in the Middle East, climbed Mount Kilimanjaro, was bitten by a deadly spider in Zanzibar and made Trappist beer at 3 AM in the Rochefort monastery. He loves to read computer logfiles while playing chess and listening to the St. Louis Cardinals. He loves Russia, his wife Jeanne, and daughters Isabelle, Sophie, and Juliet. Kenneth drinks beer and feeds the empty cans to camels.

Paper Enigma Machine




Rotor I
A E
B K
C M
D F
E L
F G
G D
H Q
I V
J Z
K N
L T
M O
N W
O Y
P H
Q X
R U
S S
T P
U A
V I
W B
X R
Y C
Z J
Rotor II
A A
B J
C D
D K
E S
F I
G R
H U
I X
J B
K L
L H
M W
N T
O M
P C
Q Q
R G
S Z
T N
U P
V Y
W F
X V
Y O
Z E
Rotor III
A B
B D
C F
D H
E J
F L
G C
H P
I R
J T
K X
L V
M Z
N N
O Y
P E
Q I
R W
S G
T A
U K
V M
W U
X S
Y Q
Z O



Rev: 2003-03-11-1047

Setup

1. Select left/center/right rotors.
2. Position initial wheel positions by sliding the indicated window letter up to the first row.

Operation

[Start at the input column at right, then work left to reflector, and then back to the right to the output column.]

1. If the ↑ notch appears in the window row, shift that rotor and the rotor to the left up one row (the Right Rotor is always shifted up one row before each letter is encoded/decoded).
2. Select letter to encode/decode in the Input column.
3. Read adjacent letter, *X*, in right hand column of the Right Rotor; select the letter *X* in the left hand column of the Rotor.
4. Repeat for Center Rotor.
5. Repeat for Left Rotor.
6. Read the adjacent letter, *R*, in the Reflector; select the *other* letter *R* in the Reflector.
7. Read adjacent letter, *Y*, in left hand column of the Left Rotor; select the letter *Y* in the right hand column of the Rotor.
8. Repeat for Center Rotor.
9. Repeat for Right Rotor.
10. Write down the adjacent letter, *Z*, in the output column.

Repeat for each letter of the message.

Example: Initial setting: I-II-III: MCK, Letter E encodes to Q.
Sample Message: QMJIDO MZWZJFJR

Many Thanks to Mike Koss for allowing us to reproduce his paper Enigma.

Visit his website at:
http://mckoss.com/crypto/enigma.htm

Bacon: A Framework for Auditing and Penetration Testing

Hernan Gips

Nowadays there is a lack of adequate frameworks to make the security consulters and pen testers life easy. A lot of separated or integrated tools like automating penenetration Testing tools improve their performance but aren't very useful for the real world consultant. Also some languages, which are not too powerful and complex like python makes others tools hard to expand to the public in general. In reality, the need for flexible, modular and extensible but also powerful kind of tool is growing in today's computing security scene due to substantial increases in the security, pen testing and code audit market. The goal of this paper is to motivate a renewed interest and present a solution based on nowadays technologies capable to handle the real world challenges and to be useful.

Bacon is an introduction to a generic framework for penetration testers and consultants as well as an Open Source modular framework. Bacon's core component is developed in C# and is able to load modules compiled to run in ECMA Common Language Infrastructure, for example C#, C++.NET, VB.NET, IronPython and others. So the core component, GUI and the modules are multi platform. These modules would run on Windows using the Microsoft CLI or Linux using Mono or another CLI implementation. Bacon's core also provides a set of facilities to generate custom reports, utility libraries and module communication. The actual development of Bacon is focused in the core component and three modules, one of them for code auditing, other for web application auditing and the last one for database auditing.

Hernan Gips worked as security consultant for 6 years in a top security consulting company in Buenos Aires, Argentina. Doing both Pentesting and Code Auditing for local and international companies. He worked as developer and architect in many different technologies including C, C++, Java and .NET.

Intro to High Security Locks and Safes

Michael Glasser
Deviant Ollam

This "Talk" will focus on the next step beyond basic locks and lock picking. You will NOT learn about basic cylinders. You will not learn how to shim a padlock. You will learn about Medeco side bars and how they've been beaten. You will learn about mul-t-lock pin-in-pin cylinders and how they've been beaten. You will learn the basics of safe manipulation. This is not a "Talk" that will teach you how to pick, the "pick-proof" locks. It will give you the foundation and methods that will allow you to understand these locks, and the concepts behind picking them. Punch and Pie will be served.

Michael D. Glasser is a Security Consultant in the New York Tri-State Area. He is currently employed by one of the worlds largest security consulting firms. Though he consults primarily on physical security, other forms of security are often part of his scope of work.

Glasser has been in the security industry for more then 10 years. He started as a technician in the field installing electronic security, and broadened his technical knowledge to cover all electronic and conventional security methods. Glasser is Licensed by New York State and a Burglar and Fire Alarm Installer, Certified as a Locksmith, and has numerous electronic security certifications. He is an active member of many local, state and national associations. He teaches classes on electronic security in the New York Area.

While paying the bills as a network engineer, Deviant Ollam's first and strongest love has always been teaching. Employed periodically at schools in the greater Philadelphia area, he is presently a student at the New Jersey Institute of Technology in the hopes of tacking some actual letters to his name and doing the professor gig full time. A fanatical supporter of First Amendment rights who believes that the best way to increase security is to publicly disclose vulnerabilities, Deviant has given lockpick demonstrations at other con events and various schools.

Inequality and Risk

Paul Graham, Y Combinator

Previous attempts to hack the connection between wealth and power have aimed mainly at eliminating economic inequality. They've all ended in disaster, because economic inequality is closely related to risk: you can't eliminate inequality without eliminating startups, and with them growth. So if you want to get rid of injustice, the place to attack is one step downstream, where wealth turns into power.

Paul Graham is the author of On Lisp, Ansi Common Lisp, and Hackers & Painters; was co-founder of Viaweb (now Yahoo Store); developed a simple Bayesian spam filter that inspired many present filters; and is one of the partners in Y Combinator.

Top Ten Legal Issues in Computer Security

Jennifer Granick, Executive Director, Center for Internet and Society, Stanford Law School

This will be a practical and theoretical tutorial on legal issues related to computer security practices. In advance of the talk, Granick will unscientifically determine the "Top Ten Legal Questions About Computer Security" that Defcon attendees have and will answer them as clearly as the unsettled nature of the law allows. While the content of the talk is audience driven, Granick expects to cover legal issues related to vulnerability disclosure, copyright infringement, reverse engineering, free speech, surveillance and civil liberties.

Jennifer Stisa Granick joined Stanford Law School in January 2001, as Lecturer in Law and Executive Director of the Center for Internet and Society (CIS). She teaches, speaks and writes on the full spectrum of Internet law issues including computer crime and security, national security, constitutional rights, and electronic surveillance, areas in which her expertise is recognized nationally.

Granick came to Stanford after almost a decade practicing criminal defense law in California. Her experience includes stints at the Office of the State Public Defender and at a number of criminal defense boutiques, before founding the Law Offices of Jennifer S. Granick, where she focused on hacker defense and other computer law representations at the trial and appellate level in state and federal court. At Stanford, she currently teaches the Cyberlaw Clinic, one of the nation's few public interest law and technology litigation clinics.

Granick continues to consult on computer crime cases and serves on the Board of Directors of the Honeynet Project, which collects data on computer intrusions for the purposes of developing defensive tools and practices and the Hacker Foundation, a research and service organization promoting the creative use of technological resources.

Surgical Recovery from Kernel-Level Rootkit Installations

Julian Grizzard

Conventional wisdom states that once a system has been compromised, it can no longer be trusted and the only solution is to wipe the system clean and reinstall. This talk goes against the grain of conventional wisdom and asks are there more efficient ways to repair a system other than complete reinstallation. Specifically, this talk will focus on the detection of and recovery from the installation of both traditional and kernel-level rootkits. Included in the presentation is a demonstration of an operating system architecture and intrusion recovery system (IRS) that is capable of recovering from some of the most prevalent rootkits seen in the wild. Prototype recovery tools will be released.

Julian Grizzard is a Ph.D. candidate in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. He received his B.S. in Computer Engineering from Clemson University and his M.S. in Electrical and Computer Engineering from the Georgia Institute of Technology. He has been studying rootkits for several years, written numerous related papers, and given many academic and research presentations. He is a member of the Honeynet Research Alliance and his research interests include kernel hacking, networking, and security.

Lost in Translation

Christian Grothoff

This presentation describes the possibilities of steganographically embedding information in the "noise" created by automatic translation of natural language documents. An automated natural language translation system is ideal for steganographic applications, since natural language translation leaves plenty of room for variation. Also, because there are frequent errors in legitimate automatic text translations, additional errors inserted by an information hiding mechanism are plausibly undetectable and would appear to be part of the normal noise associated with translation. Significantly, it should be extremely difficult for an adversary to determine if inaccuracies in the translation are caused by the use of steganography or by perceptions and deficiencies of the translation software. A prototype, Lost in Translation (LiT), will be presented.

Christian Grothoff is a Ph.D. Student in Computer Sciences at UCLA. His research areas are programming languages and security with focus on privacy enhancing technologies. He started and maintains the GNUnet, the GNU project for secure peer-to-peer networking with focus on anonymous file-sharing. Together with Krista Bennett he started the Lost in Translation (LiT) project, which explores new ideas in text steganography.

The Insecure Workstation II `bob reloaded`

Deral Heiland

The insecure workstation II `Bob Reloaded`. Exploring attack vectors within Microsoft desktop systems. A close look at third party applications that still suffer from api call vulnerabilities and how attackers can use these vulnerabilities to escalate there rights to system level . Also will be exploring this year's security research into "attacks against the local desktop login". Demonstration of desktop access without logging in.

Deral Heiland serves as a Network Security Analyst for a fortune 500 company. Mr. Heiland manages application and network vulnerability testing, Intrusion Detection Systems, controls firewall security and anti-virus efforts. With over a decade of work in the Information Technology field, Mr. Heiland has obtained several certifications including: CISSP, SSCP, CCNA, CWLSS, and CNE5.

Your Defense is Offensive

hellNbak, Resident Asshole, Nomad Mobile Research Center (NMRC)

Every Corporation in the world has run out and purchased IDS, Patch Mangement and other products that are selling security. This talk will outline ways that these so called "security products" can actually be used against an organization. Organizations should fear their poorly implemented "Security"

hellNbak has been around the IT Security industry for 13 years and is the resident trouble maker of NMRC. In his spare time he is the founder and moderator of VulnWatch (www.vulnwatch.org) and a data mangler for OSVDB (www.osvdb.org).

No Women Allowed? Exploring Gender Differences In Hacking

Thomas J. Holt, A.B.D., Department of Criminal Justice, University of North Carolina-Charlotte; currently affiliated with the Department of Criminology and Criminal Justice at the University of Missouri-Saint Louis

The President of Harvard University, Lawrence H. Summers, recently suggested the lack of women in the sciences is due to innate differences between men and women. He speculated a variety of reasons for this including genetics and social factors, and his comments created a stir among academics and the general public. While the accuracy of his statements are suspect, he raises an intriguing question in light of declining female enrollment in computer science and engineering degree programs at MIT and other universities. And if women are falling out of these fields, what is happening to the population of female hackers and security professionals? What have their experiences been up to this point? Research suggests men dominate the underground, and sociological research suggests this is attributable to social practices rather than innate sex differences. However, the female hackers' perspective has not been well documented. Furthermore, the existing literature on this issue is based largely on anecdotal rather than empirical evidence. As such, it is necessary to examine the gendered experiences of hackers to expand our knowledge of how these experiences impact individuals and their behavior.

The purpose of this talk is to introduce my research agenda to study male and female hackers, and examine variations across gender. During the talk, I will lay out fundamental theoretical concepts used to discuss the different experiences of men and women on and off-line. Then I will introduce my research proposal and call for interested individuals to participate in this study. Throughout the presentation, the audience is welcome to share their personal feelings, beliefs, and knowledge about gender and hacking. The start of an open dialogue, whether formal or informal, regarding gender differences in hacking is critical to advance our understanding of this important issue for information technology and the sciences.

Tom Holt is completing his Ph. D. in Criminology and Criminal Justice at the University of Missouri-Saint Louis. He is also an Assistant Professor in the Department of Criminal Justice at the University of North Carolina-Charlotte specializing in crime and technology. Much of his graduate career has been spent examining computer crime and cybercrime, especially hackers and hacking. His dissertation research examines the elements that compose the hacker subculture, as well as its' social organization through multiple data sources. Tom has collected various materials to that end, including interviews with active hackers. His primary goal is to understand various social aspects of hacking and the computer underground from the hacker's perspective.

Meme Mining for Fun and Profit

Broward Horne, Consultant

Technology trends are treacherous. Should you learn java or visual basic? Pay for Windows or download Linux? Will that investment in Bluetooth pay off? Or will you get suckered by a faddish book written by a fading technology guru?

You can't know the future (yet), but you can make educated guesses and tilt the odds in your favor. Meme Miner is a simple program for trend tracking. Its power lies in the business and social bandwidth concepts behind its creation.

Meme Miner shows current technology trends, but also gives an historical perspective of their past. You will NOT get a lesson in HTTP hacking in this session, but you will get practical and valuable business concepts to help survive (and perhaps prosper) in the next technology upheaval.

Broward Horne is a software developer with a diverse background, including several years as an electronic technician at Litton and Teradyne and as a sysadmin at a major University. Broward also has a business background, doing contract work for the United States Department of Transportation on experimental pen-based systems, early wireless LANs and two-dimension barcoding.

GeoIP Blocking, A Controversial But (Sometimes) Effective Approach

Tony Howlett, President, Network Security Services, Inc.

What if I told you, than in a few minutes and at no extra cost, you could be blocking up to 30% of all malware headed for your network? Sound too good to be true? Well it doesn't work for everyone and there are a lot of caveats, but it can be an effective way to eliminate a large portion of the malicious traffic aimed at your network. In this talk we will cover why you would want to GeoIP block and why it might not be a good choice for you. We will then get into the mechanics with actual IP blocks given and strategies for both full and limited GeoIP blocking. You have nothing to lose and may gain a valuable tool in your network security arsenal.

Tony Howlett is President of Network Security Services, Inc. He was previously founder and CTO of InfoHighway Communications Corp., a leading ISP and CLEC. He is a frequent speaker and writer on security, the Internet and technology. His articles have appears in SysAdmin, Security Administrator, Windows Web Solutions, Windows IT Pro, Texas Computing and Computer Currents magazines. He is also author of "Open Source Security Tools" published by Addison Westley in 2004. Type "Tony Howlett" into Google to get additional references.

The Next Generation of Cryptanalytic Hardware

David Hulton, Dachb0den Labs

Encryption is simply the act of obfuscating something to the point that it would take too much time or money for an attacker to recover it. Many algorithms have time after time failed due to Moore's law or large budgets or resources (e.g. distributed.net). There have been many articles published on cracking crypto using specialized hardware, but many were never fully regarded as being practical attacks. Slowly FPGAs (Field Programmable Gate Arrays) have become affordable to consumers and advanced enough to implement some of the conventional software attacks extremely efficiently in hardware. The result is performance up to hundreds of times faster than a modern PC.

This presentation will provide a walk through on how FPGAs work, review their past applications with crypto cracking, present basic tips and pointers to developing a fast and efficient crypto cracking design, discuss overclocking FPGAs, and analyze the future growth of FPGA hardware and it's relation to current crypto ciphers. Then, a new open source DES cracking engine will be released and demonstrated which is able to crack windows Lanman and NTLM passwords at a rate over 600,000,000 crypts per second on a single low-cost Virtex-4 LX25 FPGA and provide brute-force performance comparable to lookups on a hard-drive based rainbowtable attack.

David Hulton is one of the founding members of Pico Computing, Inc., a manufacturer of compact embedded FPGA computers and dedicated to developing revolutionary open source applications for FPGA systems. He is also one of the founding members of Dachb0den Research Labs, a non-profit security research think-tank, is currently the Chairman of ToorCon Information Security Conference and has helped start many of the security and unix oriented meetings in San Diego.

Credit Cards: Everything You have Ever Wanted to Know

Robert "hackajar" Imhoff-Dousharm, Merchant Credit Card Consultant, Hackajar Group

Identity theft is at an all time high. With businesses, universities and banks being compromised the threat is real right now. The media covers these area's but miss one important location that your most susceptible to fraud, everywhere you swipe your credit card. We will pull out all the stops to help you understand credit cards, their history and how to protect yourself. Ever wonder what was in the magnetic strip of a card? Where that information goes? Who keeps your personal information, and for how long? Who is data mining this information? Who do they sell it to? All these questions and more will be answered in this presentation Defcon 11 we talked about social engineering to steal your credit card information. Defcon 12 we gave a live example on stealing credit card data from merchant networks. Now we will show you what that information is, and how to protect yourself against fraud.

Robert "hackajar" Imhoff-Dousharm has worked in computer security for over 6 years. He has spent 2-1/2 years in the merchant credit card security field. Last year he has started his own credit card security consulting firm to focus more on securing businesses one client at a time. He also works in a SOC for a large client, insuring data integrity, availability and confidentiality. Robert has spoken at Defcon 11 & 12 in both social security and network security of credit cards in merchant environments.

Black Ops 2005

Dan Kaminsky

Another year, another batch of packet related stunts. A preview:

1. A Temporal Attack against IP
   It is commonly said that IP is a stateless protocol. This is not entirely true. We will discuss a mechanism by which IP's limited stateful mechanisms can be exploited to fingerprint operating systems and to evade most intrusion detection systems.
2. Application-layer attacks against MD5
   We will show how web pages and other executable environments can be manipulated to emit arbitrarily different content with identical MD5 hashes.
3. Realtime visualizations of large network scans
   Building on Cheswick's work, I will demonstrate tools for enhancing our comprehension of the torrential floods of data received during large scale network scans. By leveraging the 3D infrastructure made widely available for gaming purposes, we can display and animate tremendous amounts of data for administrator evaluation.
4. A High Speed Arbitrary Tunneling Stack
   Expanding on last year's talk demonstrating live streaming audio over DNS, I will now demonstrate a reliable communication protocol capable of scaling up to streaming video over multiple, arbitrary, potentially asymmetric transports.

Dan Kaminsky, also known as Effugas, is a Senior Security Consultant for Avaya's Enterprise Security Practice, where he works on large-scale security infrastructure. Dan's experience includes two years at Cisco Systems designing security infrastructure for large-scale network monitoring systems.

He is best known for his work on the ultra-fast port scanner scanrand, part of the "Paketto Keiretsu", a collection of tools that use new and unusual strategies for manipulating TCP/IP networks. He authored the Spoofing and Tunneling chapters for "Hack Proofing Your Network: Second Edition", was a co-author of "Stealing The Network: How To Own The Box", and has delivered presentations at several major industry conferences, including Linuxworld, DefCon, and past Black Hat Briefings.

Dan was responsible for the Dynamic Forwarding patch to OpenSSH, integrating the majority of VPN-style functionality into the widely deployed cryptographic toolkit. Finally, he founded the cross-disciplinary DoxPara Research in 1997, seeking to integrate psychological and technological theory to create more effective systems for non-ideal but very real environments in the field.

Passive Host Auditing

jives

Traditionally, IDS systems such as snort have been used to monitor attacks against or within a network. This talk will give the outline for turning those tools around and instead using them to audit networks. We will discuss how to identify OS's, tell who is patching, what services are being deployed (perhaps insecurely), and other methods

for policy enforcement. This discussion is ideally suited for administrators and security professionals in open and/or decentralized environments, especially those charged with auditing the network. While several signatures and sample scripts will be discussed during this talk, this is a relatively new area of auditing and network security so questions, comments and volunteers will all be welcome.

Jives has been doing computer security at a major research university for over 5 years. After initially specializing in host security he has moved into network security. In this area he has written several evidence gathering scripts. Recently he has made a hobby out of using the network to answer questions about the host.

Doing Not-For-Profit Tech:
The Hacker Foundation Year in Review

Jesse Krembs, President, The Hacker Foundation
Nick Farr (THF Treasurer)
Emerson Tan (THF Vice President)
Frazier Cunningham (THF Secretary)
Jennifer Granick (THF Legal Affairs Officer)
James Schuyler (THF East Africa Region Coordinator)
Christian Wright & William Knowles (THF Board Members)
& other select members of the Foundation Board.

Fresh from a year of grappling with Tsunamis, the IRS and building IT in Uganda, members of The Hacker Foundation will tell the story of their first year as a federally recognized non-profit organization while providing practical insight on doing charitable IT work throughout the world. Tips and tricks on everything from funding for free software projects to keeping a dust storm from killing your laptop will be presented.

The Hacker Foundation serves as a research and service organization to promote and explore the creative use of technological resources across frontiers with a global outlook.

Jesse Krembs is the Head Defcon Speaker goon, and has been involved with Defcon since 1998. He is co-founder of the Hacker Foundation and its current president. He travels widely doing radio survey work & wireless installation for Fortune 500 companies. He restores classic motorcycles and naps in his spare time.

Nick Farr spent the first decade of his career serving in non-profit management roles in academia, public radio, print journalism and computer recycling. While pursuing a new career in Public Accounting, he continues to serve in his role as Treasurer of the Hacker Foundation which he co-founded.

Jennifer Stisa Granick joined Stanford Law School in January 2001, as Lecturer in Law and Executive Director of the Center for Internet and Society (CIS). She teaches, speaks and writes on the full spectrum of Internet law issues including computer crime and security, national security, constitutional rights, and electronic surveillance, areas in which her expertise is recognized nationally.

A Linguistic Platform for Threat Development

Ben Kurtz, Imperfect Networks

Sick of hand-coding each and every exploit? The past few years have seen the rise of some generalized frameworks for the exploitation of vulnerabilities, but none of them are general-purpose enough to accommodate arbitrary hardware and network protocols. By applying programming language theory to the development of new networks attacks, we can create next-generation platforms capable of quickly handling arbitrary protocols and hardware, and exponentially reducing threat development time. The advances made in compilers in the past decades allow us to divorce ourselves from the tedious mechanics of custom-crafting network attacks and focus only on what we want the attack to do.

This new platform has serious implications for both good (rapidly adding 0-day exploits to your lab's regression testing with no programming knowledge) and for evil (allowing people with no programming knowledge to wield a database of malevolence). The Linguistic Platform can simultaneously accommodate both the generation of network traffic and the decomposition of packet captures for subsequent modification and playback. Using this system, a user can capture a malicious traffic stream in Ethereal, modify it as needed, and play it back on a live network. By deploying several clustered systems, it can even play back multi-node conversations, such as a man-in-the-middle attack. The design of new threats and the organization of threats into a database are also drastically simplified by this system.

In this talk, I will introduce a simple and incredibly powerful approach to the scripting, capture, and playback of malicious network traffic, and detail the design

goals and considerations of a Linguistic Platform for Threat Development. Some familiarity with linguistics or finite automata will be helpful, but is not required.

Ben Kurtz is a principal researcher and developer of threat generation and analysis technologies at Imperfect Networks. Earlier, he earned his Masters of Computer Science by applying language theory to the visual analysis of probe data under the DARPA DASADA program, but has since discovered that it's much easier to break something than to fix it. In other incarnations, he has worked on critical systems for power plants, passenger jets, and insurance companies. If you knew him better, this would make you nervous.

Introducing Unicornscan - Riding the Unicorn

Robert E. Lee, Founder, Dyad Labs
Jack C. Louis, Founder, Dyad Labs

Unicornscan is an open source (GPL) tool designed to assist with information gathering and security auditing. This talk will contrast the real world problems we've experienced using other tools and methods while demonstrating the solutions that Unicornscan can provide.

We will use Unicornscan to collect information from large networks, data mine the collected information, and test systems for susceptibility to specific vulnerabilities.

Some of the more interesting content includes:

- An introduction to the Scatter Connect method of TCP Connection State information tracking.
- How to get more mileage out of the information contained inside the TCP stream for OS and possibly application fingerprinting.
- How to avoid the kernel fixing packets that we have specifically created to be invalid.
- How to deliver platform specific exploits using just the information from one Target response packet (SYN/ACK).
- How to take stable working exploits and use Unicornscan as a delivery agent.

During the talk we will release a new DEFCON specific version of Unicornscan that contains many enhancements that we will demonstrate during the talk. The DEFCON version will also contain a couple of special payload configuration files not included in the standard release. To get the most out of this talk attendees should have a strong working knowledge of TCP/IP, C programming, assembly, and OS/Application fingerprinting techniques.

Robert E. Lee serves as Dyad Labs's CEO. Robert's primary roles include technology and software development, security research, and education program initiatives. Robert also serves as the Director of Projects & Resources for the Institute for Security and pen Methodologies. Robert is a key contributor to the Open Source Security Testing Methodology Manual, Unicornscan, and Cruiser (no URL yet) projects. Robert maintains his OSSTMM Professional Security Tester (OPST) & OSSTMM Professional Security Analyst (OPSA) certifications from the Institute for Security and Open Methodologies (ISECOM).

Jack C. Louis is a Senior Security Researcher for Dyad Labs. He has a background in core networking technologies, systems programming, and electronics. Jack is the lead programmer behind Unicornscan, a distributed data information engine for the the OSACE project. Jack is also the lead author of cruiser, a web application testing tool in the OSACE suite. Jack is also an ISECOM OPST & OPSA Certified Instructor.

The Dark Side of Winsock

Jonathan Levin

The Winsock SPI, or Service Provider Interface, has been a part of Winsock since the advent of version 2.0. It enables providers to extend the Winsock API transparently, by installing their own hooks and chains to application API calls. However, its formidable capabilities are not put to widespread use... aside from spyware (remember Kazaa's "sporder.dll"?).

The talk will discuss (and demonstrate) some of the more insidious uses of the SPI. From collecting connection statistics, through eavesdropping on data, or rerouting connections, with the application remaining totally oblivious!

Jonathan Levin has been involved with Information Security since the mid '90's. He has consulted for over 8 years (mostly in Israel), and trained numerous IT and security related courses, in academic as well as technical fora.

Johnny is an independent security consultant and trainer, and has worked closely with many companies, e.g. Checkpoint, NDS and M-Systems. He has first encountered the Winsock SPI back in '98 (and got to know all too intimately by writing device driver hooks

over it...), but is surprised to see that, even after almost 7 years, it has gotten little attention, despite its potent features.

Death By A Thousand Cuts - Forensics
Johnny Long, Penetration Tester

In this day and age, forensics evidence lurks everywhere. This talk takes attendees on a brisk walk through the modern technological landscape in search of hidden digital data. Some hiding places are more obvious than others, but far too many devices are overlooked in a modern forensics investigation. As we touch on each device, we'll talk about the possibilities for the forensic investigator, and take a surprising and fun look at the nooks and crannies of many devices considered commonplace in today's society. We'll look at iPods (and other MP3 players), Sony PSP devices (and other personal video products), digital cameras, printers, fax machines, all-in-one devices, dumb phones, "smart" phones, cell phones, various network devices and even wristwatches, sunglasses, pens and all sorts of other devices that contain potential evidence. For each device, we'll look at what can be hidden and talk about various detection and extraction techniques, avoiding at all costs the obvious "oh I knew that" path of forensics investigation. All this will of course be tempered with Johnny's usual flair, some fun "where's the evidence" games, and some really cool giveaways.

Johnny Long is a "clean-living" family guy who just so happens to like hacking stuff. Over the past two years, Johnny's most visible focus has been on this Google hacking "thing" which has served as yet another diversion to a serious (and bill-paying) job as a professional hacker and security researcher for Computer Sciences Corporation. In his spare time, Johnny enjoys making random pirate noises ("Yarrrrr!"), spending time with his wife and kids, convincing others that acting like a kid is part of his job as a parent, feigning artistic ability with programs like Bryce and Photoshop, pushing all the pretty shiny buttons on them new-fangled Mac computers, and making much-too-serious security types either look at him funny or start laughing uncontrollably. Johnny has written or contributed to several books, including "Google Hacking for Penetration Testers" from Syngress Publishing, which has secured rave reviews and has lots of pictures.

Google Hacking for Penetration Testers
Johnny Long, Penetration Tester

Google Hacking returns for more guaranteed fun this year at Defcon 13! If you haven't caught one of Johnny's Google talks, you definitely should. Come and witness all the new and amazing things that can be done with Google. All new for Defcon 13, Johnny reveals basic and advanced search techniques, basic and advanced hacking techniques, multi-engine attack query morphing, and zero-packet target foot printing and recon techniques. Check out Google's search-blocking tactics (and see them bypassed), and learn all about using Google to locate targets Google doesn't even know about! But wait, there's more! Act now and Johnny will throw in the all new "Google Hacking Victim Showcase, 2005" loaded with tons of screenshots (and supporting queries) of some of the most unfortunate victims of this fun, addictive and deadly form of Internet nastiness. Think you're too über to be caught in a Google talk? Fine. Prove your badness. Win the respect of the audience by crushing the live Google Hacking contest! Submit your unique winning query by the end of the talk to win free books from Syngress Publishing and other cool gear! Or don't. Just listen to your friends rave about it. Whatever.

Social Engineering Do's & Don'ts (A Female Perspective)
Beth Louis (Phen)

Social Engineering Do's and Don'ts is more informative then technical. Over the course of the lecture, I plan on going over some information you may not have thought of in your pursuits. Such as, telephone surveys, the importance of being well informed, along with basics such as the importance of both phone & social etiquette, surveillance, going undercover, corporate fraud and of course identity theft. There will be live demonstrations & explanations. This is the talk for everything you wanted to know about social engineering but were to technical to ask.

Phen has been doing social engineering since the late 1980's. Starting off by running a BBS and convincing the local ISP to give her free Internet usage to "working " at West Point Military Academy. She has used her skills to get into places such as the World Bank, Lockheed & Martin, AT&T, along with the Bank of England & other corporate and financial institutions. Although not a member, Her current affiliations are with The Ninja

Strike Force on behalf of Cult of the Dead Cow, which whom she has been working on projects with for the past 4 years. She enjoys red lipstick, black skirts and strong tequila.

The Six Year Old Hacker: No More Script Kiddies.

Kevin McCarthy

Computer use in elementary schools is problematic. Seldom are computers well integrated into the general curriculum. Often, they are used merely as instructional surrogates to "drill" skills. Particularly disturbing is the lack of exploration of the computer itself, and the culture of technology. Programming can teach vital problem solving skills, project management, respect for others work, and the value of collaboration. So why not cultivate the methods and ethics of hacking in young children? For the last 2 years I have been doing just that. Working with 6 to 12 year olds in a small Montessori school, I have begun to develop a program to encourage curiosity in our created, technological world, in the same way that their teachers encourages such curiosity in the natural world. I would like to open a discussion on the value of this approach, and the methods I employ. Perhaps I can encourage others to help cultivate the next generation of hackers.

Kevin McCarthy has worked as a system and network administrator 15 years. He is currently a network and security consultant. He teaches programming to elementary school children and encourages their natural tendencies to hack.

Old Skewl Hacking - InfraRed

Major Malfunction

Infra Red is all around us. Most of us will use an Infra Red controller on more or less a daily basis, to change the TV channel, or open a car or garage door, but how often have you thought about how it actually works? This talk will describe not only how to analyse the signals being sent by your remote, but also how to use that information to find hidden commands and reveal functions you didn't even know your systems had. You will learn how to brute force garage doors, car doors, hotel pay-per-view TV systems, take over LED signs, vending machines and even control alarm systems, using cheap or home made devices and free software...

Major Malfunction is a security professional by day, and a White Hat hacker by night. He is a good example of what happens to TheGoodGuys™ when you force them to travel, eat junk food, drink too much coffee, and stay in cheap hotels. If your hotel has a hole in it, Major Mal will find it... He has been involved in DEFCON, as a Goon, since DC5, and the computer industry since the early Eighties. He was co-founder of the world's first full time Internet pirate radio station, InterFACE, and wrote the first ever CD ripper, 'CDGRAB', disproving the industry lie that computers could not read music CDs. In his spare time, he likes to play with guns. Big guns. Little guns. As long as it goes BANG, it will be his friend, and he will love it, care for it, and feed it plenty of ammo. Let him fondle your weapon, and you'll have a friend for life...

Visual Security Event Analysis

Raffael Marty, Senior Security Engineer, ArcSight Inc

In the network security world, event graphs are evolving into a useful data analysis tool, providing a powerful alternative to reading raw log data. By visually outlining relationships among security events, analysts are given a tool to intuitively draw conclusions about the current state of their network and to respond quickly to emerging issues.

I will be showing a myriad of graphs generated with data from various sources, such as Web servers, firewalls, network based intrusion detection systems, mail servers, and operating system logs. Each of the graphs will be used to show a certain property of the dataset analyzed. They will show anomalous behavior, misconfigurations and simply help document activities in a network.

As part of this talk, I will release a tool tool that can be used to experiment with generating event graphs. A quick tutorial will show how easy it is to generate graphs from security data of your own environment.

Raffael Marty is a senior security engineer with ArcSight, the global leader in Enterprise Security Management (ESM). He initiated the Content team, holding responsibility over all the content in ArcSight's product, ranging from correlation rules to categorizations, vulnerability mappings, to visualizations and dashboards. Before joining ArcSight, he was a member of the Global Security Analysis Lab at IBM Research, where he participated in various intrusion detection related projects. His Master's thesis focused on correlating

events and testing intrusion detection systems. The resulting tool he created, Thor, can be used to generate correlation tables for multiple, heterogeneous IDS sensors. .

Meet the Fed

Jim Christy and various other Feds

A unique opportunity to surrender and confess all of your crimes to law enforcement agents from multiple federal and possibly international agencies. The "Meet the Fed" Panel is again chaired by Special Agent Jim Christy, Director of the Department of Defense Cyber Crime Institute. Jim will have on his panel representatives from:

- Department of Defense Cyber Crime Center (DoD)
- The Internal Revenue Service (IRS - always a favorite)
- General Accounting Office (GAO)
- US Postal Service
- Federal Bureau of Investigation (FBI)
- National Security Agency (NSA) (2)

If you don't want to confess yourself, you can certainly drop a dime on one of the other DEFCON attendees.

Trust Transience: Post Intrusion SSH Hijacking

Metalstorm

Trust Transience: Post Intrusion SSH Hijacking explores the issues of transient trust relationships between hosts, and how to exploit them. Applying technique from anti-forensics, linux VXers, and some good-ole-fashioned blackhat creativity, a concrete example is presented in the form of a post-intrusion transparent SSH connection hijacker. The presentation covers the theory, a real world demonstration, the implementation of the SSH Hijacker with special reference to defeating forensic analysis, and everything you'll need to go home and hijack yourself some action.

Metalstorm is a deathmetal listening linux hippy from New Zealand. When not furiously playing air-guitar, he works for linux integrator and managed security vendor Asterisk in Auckland, New Zealand. Previous work has placed him in ISP security, network engineering, linux systems programming, corporate whore security consultancy and a brief stint at the helm of a mighty installation of solaris tar. Amongst his preoccupations at the moment are the New Zealand Supercomputer Centre, wardriving-gps-visualization software that works in the southern hemisphere, and spreading debian and python bigotry.

ATM Network Vulnerabilities

Robert Morris, Former Chief Scientist, NSA

When was the last time you visited an actual human being to withdraw some spending money? In a world where most people visit computers for cash, ATM Networks have been traditionally thought of as a secure haven. Financial data theft is more of a reality than ever, but the backbone for the majority of cash to consumer transactions is not a target. I will show you why that is about to change. During my years at the NSA, I witnessed the growth of the electronic banking industry and observed many poor security design decisions as the ATM network was built. The means for authentication, the protection of data, and the methods for transferring sensitive information are just the tip of the iceberg. The ATM network is the next financial hacking pot of gold.

Robert Morris received a B.A. in Mathematics from Harvard University in 1957 and a M.A. in Mathematics from Harvard in 1958. He was a member of the technical staff in the research department of Bell Laboratories from 1960 until 1986. On his retirement from Bell Laboratories in 1986 he began work at the National Security Agency. From 1986 to his (second) retirement in 1994, he was a senior adviser in the portion of NSA responsible for the protection of sensitive U.S. information.

Hacking the Mind (Influence and NLP)

Mystic

Do you ever find yourself wondering if good social engineers and highly influential people are just born that way? Well, you might be surprised to find out that any human skill can be duplicated including being a master at influence. This is what forms the basis for a field of study known as NLP or Neuro-Linguistic-Programming. In this talk I will give an introduction to what NLP is and how it is used and will also provide you with some tools to help you better understand how you and others are influenced and how to exploit it.

Mystic is a strong believer that hacking at its core has little to do with computers and more to do with how you chose to live your life. His interests go from electronic music to poetry to encryption to designing Texas Hold'em AIs.

Ask EFF: The Year in Digital Liberties

Annalee Newitz, Policy Analyst, Electronic Frontier Foundation
Wendy Seltzer, Special Projects Coordinator, Electronic Frontier Foundation
Kevin Bankston, Staff Attorney, Electronic Frontier Foundation
Kurt Opsahl, Staff Attorney, Electronic Frontier Foundation
Seth Schoen, Staff Technologist, Electronic Frontier Foundation

Get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, a digital civil liberties group fighting for freedom and privacy in the computer age. This session will include updates on current EFF issues such as DRM, file-sharing, spyware, the USA-Patriot Act, and bloggers' rights. But over half the session will be given over to question-and-answer, so it's your chance to ask the panelists questions about issues important to you.

Annalee Newitz is EFF's Policy Analyst. She writes policy recommendations and white papers, including recent papers on the dangers of EULAs, the problems with anti-spam regimes, and how to blog anonymously. Her special areas of interest are free speech, anonymity, network regulation, and expanding the public domain. The recipient of a Knight Science Journalism Fellowship in 2002, she writes a syndicated weekly column called Techsploitation and is a contributing editor at Wired magazine.

Kurt Opsahl is a Staff Attorney with the EFF focusing on civil liberties, free speech and privacy law. Before joining EFF, Opsahl worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters, including working on Kelly v. Arribasoft, MGM v. Grokster and CoStar v. LoopNet. For his work responding to government subpoenas, Opsahl is proud to have been called a "rabid dog" by the Department of Justice.

Seth Schoen created the position of EFF Staff Technologist, helping other technologists understand the civil liberties implications of their work, EFF staff better understand the underlying technology related to EFF's legal work, and the public understand what the technology products they use really do. Schoen comes to EFF from Linuxcare, where he worked for two years as a senior consultant. While at Linuxcare, Schoen helped create the Linuxcare Bootable Business Card CD-ROM.

Wendy Seltzer is Special Projects Coordinator with the EFF, specializing in intellectual property and free speech issues. As a Fellow with Harvard's Berkman Center for Internet & Society, Wendy founded and leads the Chilling Effects Clearinghouse, helping Internet users to understand their rights in response to cease-and-desist threats. Prior to joining EFF, Wendy taught Internet Law as an Adjunct Professor at St. John's University School of Law and practiced intellectual property and technology litigation with Kramer Levin Naftalis & Frankel in New York.

Kevin Bankston, an attorney specializing in free speech and privacy law, is the EFF's Equal Justice Works/Bruce J. Ennis Fellow for 2003-05. His fellowship project focuses on the impact of post-9/11 anti-terrorism laws and surveillance initiatives on online privacy and free expression. Before joining EFF, Kevin was the Justice William J. Brennan First Amendment Fellow for the American Civil Liberties Union in New York City. At the ACLU, Kevin litigated Internet-related free speech cases, including First Amendment challenges to both the Digital Millennium Copyright Act (Edelman v. N2H2, Inc.) and a federal statute regulating Internet speech in public libraries (American Library Association v. U.S.).

Causing the Law

Mark Pauline, founder of SRL

Survival Research Laboratories (SRL) was founded by Mark Pauline in November 1978. Since its inception, SRL has operated as an organization of creative technicians dedicated to re-directing the techniques, tools, and tenets of industry, science, and the military away from their typical manifestations in practicality, product or warfare. Since 1979, SRL has staged over 45 mechanized presentations in the United States and Europe. Each performance consists of a unique set of ritualized interactions between machines, robots, and special effects devices, employed in developing themes of socio-political satire. Humans are present only as audience or operators. More information can be found at www.srl.org

Mark Pauline passion is legal, but only in the places he has never been. Follow him through his history of causing the law.

Bypassing Authenticated Wireless Networks

Dean Pierce
Brandon Edwards
Anthony Lineberry

As the demand for mobile internet access increases, more and more public wireless access points are becoming available for general usage. Unfortunately, as awareness of these access points increases, some companies have been capitalizing on the idea, charging monthly and hourly rates.

This talk discusses methods of silently bypassing current implementations of authenticated wireless networks. An automated proof of concept tool is released and explained. Some theoretical methods of authentication that might be implemented in the future are also discussed.

Both Dean and Brandon are undergraduates in computer science at Portland State University. Both have very strong interests in the fields of wireless communications, network security, and cryptanalysis. They are also active members of pdx2600.

Anthony currently works for Logic Library Inc as a software engineer developing static binary analysis software. He has been active in computer and network security since early high school. His main interests lie in kernel development, binary reverse engineering, and embedded systems.

Suicidal Linux

Bruce Potter, the Shmoo Group

I spend a lot of my time shooting at random targets. Last year I was on a Bluetooth holy war, trying to raise awareness of Bluetooth security (or lack therein). My talk at BH 04 was actually a two day experiment using Bluetooth to track attendees around the conference (code available from bluetooth.shmoo.com). While the technology was simple, the message needed to get out. Bluetooth enabled phones are dangerous and are flying under the security industry's radar screen.

Fast forward a year, and the situation is much better. Bluetooth security is getting more and more coverage and research (www.trifinite.org is a great site for BT security issues), and people are (finally) getting scared. So I decided to shift gears into a bigger hornet's nest... The holy war of Operating System security.

No, not the standard issue "OpenBSD is uber secure, Windows sucks" discussion. Rather, I've been focusing on the long term impact of each of these operating systems on the security of enterprise networks and the Internet as a whole. Any reasonable tech geek can be trained to lock down a host. Give them a checklist and some procedures and lock it down and *boom* a secure host. However, while that host may be secure today, what are the differences in long term security between the major operating systems.

As it turns out, a lot of the long term security issues revolve around the development method used to develop the OS. Windows is designed as one big system, and to some extent the BSD's are as well. But Linux... Linux is designed with duct tape in mind. Linux distros are held together with spit and tape, and the ramifications on security are dire. I've been gathering data from mail lists, looking at code, and talking to people running big systems in an attempt to figure out how bad things really are. I'm sure many of you will find this talk inflammatory, and that's a good thing. "Knowing is half the battle." ... even if you don't want to hear it.

The Shmoo Group is a non-profit think-tank comprised of security professionals from around the world who donate their free time and energy to information security research and development. They get a kick out of sharing their ideas, code, and stickers at DefCon. Whether it's mercenary hacking for CTF teams, lock-picking, war-flying, or excessive drinking, TSG has become a friendly DefCon staple in recent years past. Visit www.shmoo.com for more info.

Shmoo-Fu: Hacker Goo, Goofs, and Gear with the Shmoo

Bruce Potter, Beetle, CowboyM, Dan Moniz, Rodney Thayer, 3ricj, Pablos all speaking on behalf of the Shmoo Group

Last Summer, they dared to make a Wi-Fi sniper rifle that fried their eyeballs and scared the crap out of UPS. They built a robot that owned your Mom's access point and showed you the password to her underwear drawer, too. Last Winter, they ran up a $3000 bar tab at a nightclub in D.C. with several hundred ShmooCon attendees—then donated just as much to EFF for shits and grins. This DefCon, the Shmoo Group brings you a slew of hacker goo, goofs, and gear to go with your shiny new "Notice to Law Enforcement" stickers. Can you resist? Probably. Will you? Nope. Why? Because they

have cool shit all over again. IDN fallout and homograph attacks on personal identities thanks to 3ricj. Hot models wearing spy actionwear designed by Pablos—fresh from his ninja lair of alien technology. Revving up rainbow tables with Dan "Don't Be Crazy" Moniz. New Wi-Fi kung-fu with "Rogue Squadron" and EAP-peeking by Beetle. Rodney Thayer explains how to blow $1 MILLION on commercial security shtuff and still get owned by a grade-school punk addicted to Xbox. CowboyM returns to show off new geeky tactical gear designed for close-quarters wireless combat—do NOT try this at home, kids, and certainly not inside a Faraday cage. Finally, because you've all been waiting for it, Bruce Potter pours gasoline on his security model self and lights a fucking match! Mo' better and with no blow-up dolls, the Shmoo Group returns to rant on recent projects and review new ones. Rated R for strong violence, adult situations, disturbing images, nudity, language, and epic warfare.

Assymetric Digital Warfare

Roberto Preatoni (aka Sys64738)
Fabio Ghioni

The speech will be intended to let the attendees understand where and how the digital conflicts are conducted today but we will dig deeply into the future. We will take as example the US Army program F.C.S. (Future Combat System) as the perfect example on how a developed superpower might carry on a super-advanced war program, all based on combat computer systems and networks that control unmanned vehicles as well as wheeled combat drones, to discover at the end that the adoption of such systems might introduce conceptual vulnerabilities that a wise enemy might exploit by means of hacking.

Roberto Preatoni (aka Sys64738): 37, is the founder of the defacement/cybercrime archive Zone-H (www.zone-h.org)as well as its key columnist. He's also CEO of an International ITsec company (Domina Security). He has been globetrotting, lecturing in several ITsec security conferences, including Defcon in the US. He has been interviewed by several print and online newspapers where he shares his experiences relating to cyberwar and cybercrimes. A man with different opinions than the usual.

Fabio Ghioni is advisor to several Multinational Corporations as well as Governments. He is the leading expert in the field of information security, competitive intelligence and intrusion management in an asymmetric environment. As consultant to several different Government institutions he has been the key to the solution of several terrorism cases in the past. His key fields of research range from mobile and wireless competitive security to the classification of information and forensics technologies applied to identity management and ambient intelligence.

Pen-testing the Backbone

Raven, NMRC

Despite its crucial importance, the network backbone is often ignored or exempted from security testing. This talk will cover how to sanely and effectively perform a pen-test against routers, switches, and similar network infrastructure equipment. Avenues of attack will range from the physical to the routing protocol-based, from the local to the remote, and suggested mitigation measures will also be discussed.

Raven splits her time between network engineering and security testing, and often tries to fuse the two, to varying degrees of success. She is equally fond of building networks for ISPs and breaking them nicely. In her Copious Spare Time, she contributes to network security books, mangles for OSVDB, kicks other people's crypto implementations, and enjoys ill-advised adventures.

Licensing Agreements 101: The Creative Commons License

Jim "FalconRed" Rennie

This talk will give some quick background on the Creative Commons license—why exactly it was created and who created it. More importantly, this talk will dissect the "lawyer" version of the license and explain some of the key terms hidden from the average user. Finally, this talk will discuss ways to maximize your protection under the license and protect your content from possible legal pitfalls.

Jim "FalconRed" Rennie is currently a law student in New York City. Previously, he spent several years as a Software Engineer at two Seattle-area companies. While in Seattle, he met up with the infamous GhettoHackers, which probably shortened his life expectancy by several years. Jim has been attending DefCon long enough to know who not to piss off.

Forensic Data Acquisition Tools

RS

Proper recovery of evidence can be critical to a successful investigation or prosecution. This talk focuses on the different tools and techniques that are used by US Law Enforcement to get an uncontaminated copy of digital evidence from a suspect machine. The goal of this presentation is to teach not only how to copy all the data from a suspect machine, but also to instruct on how to make sure that any evidence collected can be used in court. Both hardware and software based forensic acquisition tools will be covered, with the various strengths and weaknesses of each product discussed.

RS investigates financial fraud within medical environments. Duties include participating in the execution of search warrants to recover computer base evidence. Because of the sensitivity of the medical data to be seized and liability issues involved, forensic images of suspect systems must be made quickly, on-site, in production medical environments, with minimal disruption to patient care.

Hacking Windows CE

San, NSFocus Corporation & XFocus Team

Security threats to PDAs and mobiles have become more and more serious. This presentation will show a buffer overflow exploitation example in Windows CE. It will cover some knowledge about ARM architecture and memory management, the features of processes and threads of Windows CE. It also will show how to write a shellcode in Windows CE (including some knowledge about decoding shellcode of Windows CE with ARM processor), and a live attack demonstration.

San is a security researcher, who has been working in the Research Department of NSFocus Information Technology (Beijing) Co., Ltd for more than three years. He's also the key member of XFocus Team.

His focus is on researching and analysing application security, and he's also the main author of "Network Penetration Technology" (Chinese version book).

Why Tech Documentaries are Impossible (And why we have to do them anyway.)

Jason Scott

Documentaries have a place in telling the history and story of many different cultures and events, but documentaries about technical subjects tend to run into common problems: too light, too wrong, too hated. Is the patient terminal? Can you create a film that is both informative and of interest to a general audience?

Having spent 4 years creating a tech documentary of his own on the era of the Dial-up Bulletin Board system, Jason Scott of textfiles.com talks about what unique challenges exist in the film medium for telling a highly technical story, as well as what choices had to be made throughout production. The talk will be illustrated with sequences from the resultant five and a half hour BBS Documentary Mini-series.

Jason Scott has been full-bore collecting history of BBSes and computer culture for 20 years, with the last four being split equally between his BBS history site textfiles.com and his documentary on Dial-up Bulletin Boards, "BBS: The Documentary". With over 200 interviews and 250 hours of footage, this project overtook his life for a very long time and in a very large way. His hobbies include gardening and enjoying civil liberties.

Automation - Deus ex Machina or Rube Goldberg Machine?

Sensepost

How far can automation be taken? How much intelligence can be embodied in code? How generic can automated IT security assessment tools really be? This presentation will attempt to show which areas of attacks lend themselves to automation and which aspects should best be left for manual human inspection and analyses.

SensePost will provide the audience a glimpse of BiDiBLAH - an attempt to automate a focused yet comprehensive assessment. The tool provides automation for:

- Finding networks and targets
- Fingerprinting targets
- Discovering known vulnerabilities on the targets
- Exploiting the vulnerabilities found
- Reporting

Roelof Temmingh is the Technical Director of SensePost where his primary function is that of external penetration specialist. Roelof is internationally recognized for his skills in the assessment of web servers. He has written various pieces of PERL code as proof of concept for known vulnerabilities, and coded the world-first anti-IDS web proxy "Pudding". He has spoken at many International Conferences and in the past year alone has been a keynote speaker at SummerCon (Holland) and a speaker at The Black Hat Briefings. Roelof drinks tea and smokes Camels.

Haroon Meer is currently SensePost's Director of Development (and coffee drinking). He specializes in the research and development of new tools and techniques for network penetration and has released several tools, utilities and white-papers to the security community. He has been a guest speaker at many Security forums including the Black Hat Briefings. Haroon doesnt drink tea or smoke camels.

Charl van der Walt is a founder member of SensePost. Charl has a number of years experience in Information Security and has been involved in a number of prestigious security projects in Africa, Asia and Europe. He is a regular speaker at seminars and conferences nationwide and is regularly published on internationally recognized forums like SecurityFocus. Charl has a dog called Fish.

Building WarDriving Hardware Workshop

Matthew L. Shuchman ("Pilgrim"), Founder & National Security Advisor, WarDrivingWorld.com

WarDriving is becoming a popular sport among hackers and DEFCON attendees, and WiFi site surveying has become an important tool for the IT security professional. This workshop will describe the basic equipment required for WarDriving and WiFi site surveying. There will be a brief presentation on the benefits and features of different types of WiFi hardware, adapter cards, chipsets, cables, pigtails, and antennas. The session will include an overview of the design and performance characteristics of different types of antennas. A primary focus of the workshop will be to show the participants how to select the components and parts required and how to construct their own cantenna (directional) and spider (omnidirectional) antennas.

Matthew L. Shuchman (Pilgrim) began his life as a hacker in the days of punch cards, ALGOL and FORTRAN. Mr. Shuchman is a founder of WarDrivingWorld.com, a web-based retailer of WarDriving and extended range WiFi hardware and a published author on business and the need for data security, see: McGrawHill/AMACOM, "The Art of the Turnaround". Mr. Shuchman is an experienced public speaker both at conferences, TV, and radio.

Legal and Ethical Aspects of WarDriving

Matthew L. Shuchman ("Pilgrim"), Founder & National Security Advisor, WarDrivingWorld.com
Frank Thornton, Blackthorn Systems ("Thorn")
Robert V. Hale II, Lawyer

This is a proposal for a panel discussion on the legality of accessing WiFi signals without the permission of the owner and will include a review of the legal and ethical issues presented by freely available WiFi both to the owner of the AP and to the users.

Included in the panel will be a presentation of recent cases involving WiFi access, WarDriving, and theft of data by WiFi, as well as a review of the Federal laws that cover use and misuse of WiFi including the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA.)

The panel members hope is that by presenting some of the legal and ethical issues that we can take the first steps towards guidelines for ethical conduct while WarDriving (and Bluesnarfing.)

The panel chairperson and organizer is Matthew L. Shuchman (Pilgrim,) who began as a hacker in the days of punch cards. Mr. Shuchman is a founder of WarDrivingWorld.com, a web-based retailer of WarDriving and extended range WiFi hardware and a published author on business and the need for data security, see: McGrawHill/AMACOM, "The Art of the Turnaround".

Mr. Shuchman has obtained commitments from two other panel members: Frank Thornton (Thorn) who runs a wireless technology consulting firm, Blackthorn System.

Thorn is the co-author of "WarDriving; Drive, Detect, Defend", and a retired member of the law enforcement community.

Robert V. Hale II, San Francisco-based lawyer, author of the recent article"Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet," and advisor to the

Cyberspace Committee of the California Bar. We are waiting for commitments from at least one other potential panel member.

The NMRC Warez 2005 Extravaganza

Simple Nomad, NMRC
NMRC Collective: HellNBak, Disturbing; ertia, Hacker; Weasel, Hacker; jrandom, Hacker; MadHat, Hacker

Lock up your children and mid-sized barnyard animals, NMRC is coming to DEFCON13. From their underground bunker located somewhere in North America, NMRC will emerge with your basic shitload of handy tools and toys, geared for helping the humble hacker in everyday chores. Look for crypto, utilities, and other hackerish tools to bring your hacker dreams alive. Most of these tools are being presented for the first time at DEFCON.

Nomad Mobile Research Centre (NMRC) is a hacker collective, and has been around since 1996. NMRC has released numerous papers, advisories, FAQs, and tools over the years, and believes that hackers have something good to give to society.Unfortunately most of the world doesn't believe in their definition of "good".

NMRC has distinguished itself in the realm of hackerdom in the following ways over other hacker groups: 1) They maintain friends of all hat colors; 2) They were the first hacker group to spell Centre with an "e" on the end; and 3) They live to hack and hack to live, unless of course they find free pr0n.

"Shadow Walker"—Raising The Bar For Rootkit Detection

Sherri Sparks
Jamie Butler, Director of Engineering, HB Gary

Last year at Black Hat, we introduced the rootkit FU. FU took an unprecedented approach to hiding not previously seen before in a Windows rootkit. Rather than patching code or modifying function pointers in well known operating system structures like the system call table, FU demonstrated that is was possible to control the execution path indirectly by modifying private kernel objects in memory. This technique was coined DKOM, or Direct Kernel Object Manipulation. The difficulty in detecting this form of attack caused concern for anti-malware developers. This year, FU teams up with Shadow Walker to raise the bar for rootkit detectors once again. In this talk we will explore the idea of memory subversion. We demonstrate that is not only possible to hide a rootkit driver in memory, but that it is possible to do so with a minimal performance impact. The application (threat) of this attack extends beyond rootkits. As bug hunters turn toward kernel level exploits, we can extrapolate its application to worms and other forms of malware. Memory scanners beware the axiom, 'vidre est credere' . Let us just say that it does not hold the same way that it used to.

Sherri Sparks is a PhD student at the University of Central Florida. She received her undergraduate degree in Computer Engineering and subsequently switched to Computer Science after developing an interest in reverse code engineering and computer security. She also holds a graduate certificate in Computer Forensics. Currently, her research interests include offensive / defensive malicious code technologies and related issues in digital forensic applications.

Jamie Butler is the Director of Engineering at HBGary, Inc. specializing in rootkits and other subversive technologies. He is the co-author and a teacher of "Aspects of Offensive Rootkit Technologies" and co-author of the upcoming book "Rootkits: Subverting the Windows Kernel" due out late July. He holds a MS in CS from UMBC and has published articles in the IEEE IA Workshop proceedings, Phrack, USENIX login, and Information Management and Computer Security. Over the past few years his focus has been on Windows servers concentrating in host based intrusion detection and prevention, buffer overflows, and reverse engineering. Jamie is also a contributor at rootkit.com.

DIRA: Automatic Detection, Identification, and Repair of Control-Hijacking Attacks

Alexey Smirnov, Student, SUNY Stony Brook
Tzi-cker Chiueh, Professor, SUNY, Stony Brook

Buffer overflow attacks are known to be the most common type of attacks that allow attackers to hijack a remote system by sending a specially crafted packet to a vulnerable network application running on it. A comprehensive defense strategy against such attacks should include (1) an attack detection component that determines the fact that a program is compromised and prevents the attack from

further propagation, (2) an attack identification component that identifies attack packets and generates attack signatures so that one can block such packets in the future, and (3) an attack repair component that restores the compromised application's state to that before the attack and allows it to continue running normally. Over the last decade, a significant amount of research has been vested in the systems that can detect buffer overflow attacks either statically at compile time or dynamically at run time. However, not much effort is spent on automated attack packet identification or attack repair. We present a unified solution to the three problems mentioned above. We implemented this solution as a GCC compiler extension called DIRA that transforms a program's source code so that the resulting program can automatically detect any buffer overflow attack against it, repair the memory damage left by the attack, and generate the attack signature. We used DIRA to compile several network applications with known vulnerabilities and tested DIRA's effectiveness by attacking the transformed programs with publicly available exploit code. The DIRA-compiled programs were always able to detect the attacks, produce attack signatures, and most often repair themselves to continue normal execution. The automatically produced signatures are context-aware as they describe all attack packets and accurate because each of the packets is described as a regular expressions. To the best of our knowledge DIRA is the first system capable of producing accurate attack signatures from a single attack instance and performing post-attack repair.

Related tools: GCC, http://gcc.gnu.org

Project home page: http://www.ecsl.cs.sunysb.edu/dira

Alexey Smirnov is a PhD student in the department of Computer Science at Stony Brook University. His is broadly interested in computer security, operating systems, and networks. He has been working on various systems research projects in the past such as Repairable Database Systems and DIRA.

Dr. Tzi-cker Chiueh is a Professor in the Computer Science Department of Stony Brook University, and the Chief Scientist of Rether Networks Inc. He received an NSF CAREER award in 1995, and has published over 130 technical papers in refereed conferences and journals in the areas of operating systems, networking, and computer security. He has developed several innovative security systems/products in the past several years, including SEES (Secure Mobile Code Execution Service), PAID (Program Semantics-Aware Intrusion Detection), DOFS (Display-Only File Server), and CASH.

Attacking Web Services: The Next Generation of Vulnerable Apps

Alex Stamos, Founding Partner, iSEC Partners, LLC

Scott Stender, Founding Partner, iSEC Partners, LLC

Web Services represent a new and unexplored set of security-sensitive technologies that have been widely deployed by large companies, governments, financial institutions, and in consumer applications. Unfortunately, the attributes that make web services attractive, such as their ease of use, platform independence, use of HTTP and powerful functionality, also make them a great target for attack.

In this talk, we will explain the basic technologies (such as XML, SOAP, and UDDI) upon which web services are built, and explore the innate security weaknesses in each. We will then demonstrate new attacks that exist in web service infrastructures, and show how classic web application attacks (SQL Injection, XSS, etc…) can be retooled to work with the next-generation of enterprise applications.

The speakers will also demonstrate some of the first publicly available tools for finding and penetrating web service enabled systems.

Alex Stamos is a founding partner of iSEC Partners, LLC, a strategic digital security organization, with several years experience in security and information technology. Alex is an experienced security engineer and consultant specializing in application security and securing large infrastructures, and has taught many classes in network and application security.

Scott Stender is a founding partner of iSEC Partners, LLC, a strategic digital security organization. Prior to iSEC, Scott worked as an application security analyst with @stake where he led and delivered on many of @stake's highest priority clients.

Hacking Google AdWords

StankDawg

The AdWords program is an advertising system used by Google. It is a pay-per-click system like may others but Google doesn't give it the attention to design that it deserves. Not only does Google take some liberties with the Terms of Service and

what they allow and don't allow in the program, but also have several flaws in the logical design of the system. There are several loopholes in this system and they will be explained and demonstrated with proof of concepts for every example.

StankDawg is a senior programmer/analyst who has worked for Fortune 500 companies and large universities. He is a staff writer for 2600 Magazine, blacklisted411, and numerous websites. He has given presentations at HOPE, Interz0ne, and other local venues and has also appeared on television. He is founder of "The Digital Dawg Pound" (the DDP) which is a group of white-hat/gray-hat hackers who produce their own magazine, radio shows, TV show, and numerous other projects at www.binrev.com/

The Revolution Will Not Be Copyrighted: Why You Should Care About Free Culture

Elizabeth Stark, freeculture.org
Fred Benenson, freeculture.org

The purpose of this paper is to explain and introduce the free culture movement and organization to the hacker community. We make the case that hackers should not only care about the ideas of free culture in the literal sense in that we seek to protect technological and digital rights, but also in a broader cultural sense. The idea of using and reusing bits of culture(the goal in a free culture) parallels the central tenets of the hacker ethos where manipulation, reuse, and recontextualization are essential. To that end, we'll show some compelling examples of art and music that we consider to be culture hacking. From reengineered Nintendo cartridges to electronic albums consisting almost totally of samples to an early 20th century modernist Mona Lisa hack, we'll demonstrate that some of the most innovative and radical cultural works are also the most derivative. We also intend to emphasize the significance of political and social action in order to maintain an environment of innovation and progress. There are highly significant cultural and technological issues that need to be addressed in society and we cannot stand by passively while leaving the control in the hands of the government, corporations, and other entities. In essence, free culture is deeply ingrained in the hacker ideal.

Elizabeth Stark is the main law student of freeculture.org. She went to Brown University and is currently attending Harvard Law School, where she is involved with the Berkman Center for Internet and Society on such issues as the digital media project, internet filtering reports, and drafting an Internet and technology law casebook. She is also an editor of the Harvard Journal of Law Technology, soon to be a Teaching Assistant in Cyberlaw, and conducts research for Professor Jonathan Zittrain. Elizabeth has worked and studied in such places as Berlin, London, Paris, and Singapore, is highly interested in the impact of technology on digital culture, and is (semi-) obsessed with electronic music. She is spending the summer as a legal intern at the EFF, where she gets to think about such issues 24/7.

Fred Benenson graduated in May with honors from New York University's with a major in Philosophy and a minor in Computer Science. He founded the official NYU chapter of the national student organization freeculture.org. He has worked professionally as a graphic designer, web programmer, and IT technician and owns at least one DeCSS shirt. When he's not involving himself in the future of intellectual property rights (or lack thereof), he likes to take pictures for his photoblog http://fasinphotoblog.com, solve the cube, and listen to copious amounts of electronic music. He is working as a Free Culture intern this summer at Creative Commons.

End-to-End Voice Encryption over GSM: A Different Approach

Wesley Tanner
Nick Lane-Smith

Where is end-to-end voice privacy over cellular? What efforts are underway to bring this necessity to the consumer? This discussion will distill for you the options available today, and focus on current research directions in technologies for the near future.

Cellular encryption products today make use of either circuit switched data (CSD), or high latency packet switched networks. We will discuss the advantages and disadvantages of these services, focusing on details of GSM cellular channels specifically. The highlight will be our current research project: encrypted voice over the GSM voice channel. We'll dig into how this works, and why it is useful.

This talk will touch on some fundamentals of modem design, voice codecs, GSM protocol basics, cryptographic protocols for voice links, and a bunch of other interesting stuff. There will be demonstrations with MATLAB/Octave and C, and we will provide some fun code to experiment with.

Wes is a systems engineer at a software-defined radio company in San Diego, California. He holds a B.S. in Electrical Engineering from Rensselaer Polytechnic Institute.

Nick is a security engineer at an innovative computer company. He holds a B.S. in Computer Science from the University of California, Santa Barbara. He is currently unreachable in Antigua, so I suppose I could say anything here. I won't.

Recapturing the Revolutionary Heart of Hacking

Richard Thieme, ThiemeWorks

A revolutionary program for preparing the future using past models of creativity and ingenuity. Deeply personal and implicitly political, this talk illuminates the potentials and possibilities of hacking in a transparent society, a surveillance society, a society that neutralizes dissent.

It defines identity hacking as a transformational process requiring all of our resources and skills. Identity hacking is alive in an underground now that is gathering itself for a defiant refusal to be captured and managed. That revolutionary heart is recaptured in the willingness to understand the mechanics of reinvention and to commit ourselves to a higher code or path than the broken options offered by a consumer society in a globalized world tilted far to the right.

Hackers in the future will have to be wily and guiltless, transparent and duplicitous, treacherous and faithful. They must know how to live in this world but never surrender, they must learn how to splice multiple possibilities into a single destiny in the moment of execution. That moment, fusing self-transcendence and action, is the revolutionary heart of hacking. It is also a means of practice for a trans-planetary quest.

Richard Thieme (www.thiemeworks.com) is an author and professional speaker focused on the deeper implications of technology, religion, and science for twenty-first century life. He has spoken for Def Con for ten years and Black Hat for eight as well as for other venues ranging from ShmooCon, ToorCon, and AUSCERT to the Pentagon, the FBI, and the US Department of the Treasury. His internet columns, "Islands in the Clickstream," are widely read and were collected and published by Syngress Publishing in June 2004. Since then he has published a dozen short stories including "The Geometry of Near," a hacker tale published online by Phrack and included in the anthology CyberTales: Live Wire. A short story collection, "More Than a Dream: Stories of Flesh and the Spirit" is coming soon and he is writing a novel, "The Necessity for Invention", which includes the adventures of Don Coyote and Pancho Sanchez, two wily hackers.

Physical Security Bypass Techniques: Exploring the Ethics of Full Disclosure

Marc Weber Tobias, Investigative Law Offices, Security.org
Matt Fiddler

Recent public disclosures detailing physical lock and safe bypass techniques have raised consumer awareness detailing the efficacy of the hardware that protects some of our most important assets. This talk will address the ethics of full-disclosure, the liability for failure to disclose, and the impact of public dissemination. Demonstrations and new discoveries of lock bypass techniques will be reviewed.

Marc Weber Tobias is an Investigative Attorney and polygraph examiner in the United States. He has written five law enforcement textbooks dealing with criminal law, security, and communications. Marc Tobias was employed for several years by the Office of Attorney General, State of South Dakota, as the Chief of the Organized Crime Unit. As such, he directed felony investigations involving frauds as well as violent crimes.

Matt Fiddler leads a Threat Management Team for a large Fortune 500 Company. Mr. Fiddler's research into lock bypass techniques have resulted in several public disclosures of critical lock design flaws. Mr. Fiddler began his career as an Intelligence Analyst with the United States Marine Corps. Since joining the commercial sector in 1992, he has spent the last 13 years enhancing his extensive expertise in the area of Unix and Network Engineering, Security Consulting, and Intrusion Analysis.

The Internet's March of Folly: How, from ARPA to WSIS, Internet Governance Has Consistently Pursued Policies Contrary To Its Self Interest.

Paul Vixie

Paul Vixie has been contributing to Internet protocols and UNIX systems as a protocol designer and software architect since 1980. Early in his career, he developed and introduced sends, proxynet, rtty, cron and other lesser-known tools.

Today, Paul is considered the primary modern author and technical architect of BINDv8 the Berkeley Internet Name Domain Version 8, the open source reference implementation of the Domain Name System (DNS). He formed the Internet Software Consortium (ISC) in 1994, and now acts as Chairman of its Board of Directors. The ISC reflects Paul's commitment to developing and maintaining production quality open source reference implementations of core Internet protocols. Vixie is currently the CTO of Metromedia Fiber Network Inc (MFNX.O).

Along with Frederick Avolio, Paul co-wrote "Sendmail: Theory and Practice" (Digital Press, 1995). He has authored or co-authored several RFCs, including a Best Current Practice document on "Classless IN-ADDR.ARPA Delegation" (BCP 20). He is also responsible for overseeing the operation of F.root-servers.net, one of the thirteen Internet root domain name servers.

Hackers and the Media- Misconceptions and Critical Tools To Combat Them

Patty L. Walsh/ Muckraker, Freelance Journalist Greenspun Media Group

Ever wonder what to do with the media when it seemingly (and definitely) reports inaccuracies with regard to hackers and hacking in general? Fed up with the constant misconceptions you feel the media has of hackers? What is to be done? This forum shall act as an interactive discussion on the misconceptions between hackers and the media, what to do in order to protect yourself, ho to handle the media and your (as well as the media s) constitutional and legal rights. There shall be a special surprise at the end for those in dire need of alleviation their stress towards? The Media.

Patty L. Walsh has been a political junkie since she was a child. She currently attends UNLV as a Senior, and is majoring in Political Science with emphasis on International Relations; along with a minor in Communications. She has written for The Las Vegas Review-Journal, Las Vegas Mercury, Las Vegas Tribune, Las Vegas CityLife, The UNLV newspaper, and currently is a freelance journalist for Greenspun Media Group. She also is a Production Assistant and DJ for KUNV 91.5 FM in Las Vegas. Walsh intends to become an international correspondent, and has many qualms with the media (except for BBC and Reuters, most of the time). She has attended DefCon since DC10, where she wrote about the media misconceptions of hackers as an intern for the Las Vegas Mercury.

DR. LINTON WELLS II, Assistant Secretary of Defense for Networks and Information Integration / CIO

Dr. Linton Wells, II was named Principal Deputy Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I) on August 20, 1998, and serves in that capacity in the C3I successor organization, Networks and Information Integration (NII). In addition, Dr. Wells serves as Acting Deputy Assistant Secretary of Defense for Spectrum, Space, Sensors, and Command, Control, and Communications (DASD (S3C3)).

Prior to this, Dr. Wells served the Office of the Under Secretary of Defense (Policy) from July 1991 to June 1998, concluding most recently as the Deputy Under Secretary of Defense (Policy Support).

Trends in Licensing of Security Tools

Chuck Willis, Senior System Security Engineer

Do you think that all those tools you download for security testing are free? Well, they may be free of cost for some uses, but the licenses of many tools commonly used by the security community are getting more restrictive and complicated. This interactive discussion will look at the current state of security tool licensing and also look at where this field may be headed. Specific examples of license restrictions in many commonly used tools will be presented in order to illustrate the current trends and also help tool users in the audience navigate the bumpy road of security licensing issues and stay on the right side of the law. Also discussed will be possible actions for tool users, tool authors, and others to make tool licensing simpler in the future.

Chuck Willis received his M.S. in Computer Science from the University of Illinois at Urbana-Champaign in 1998. After graduation, he spent five years conducting computer forensics and network intrusion investigations as a U.S. Army Counterintelligence Special Agent. Chuck is now conducting Penetration Testing and Vulnerability Assessments as a security contractor. Chuck has previously spoken at the Black Hat Briefings USA and the IT Underground security conference in Europe. Chuck has contributed to several open source security software projects and is a member of the Open Web Application Security Project, a CISP, and a Certified Forensic Computer Examiner. Chuck's past presentations are available on his Web site at www.securityfoundry.com/

Attacking Biometric Access Control Systems
Zamboni, Researcher, Miskatonic Research Labs

This talk explores how to attack biometric authentication systems, primarily physical access control systems. Previous literature on this topic has focused on attacking a biometric reader in the form of spoofing a biometric trait. This presentation goes a step further and provides a general methodology for attacking on complete biometric systems. The methodology can be applied to any biometric system and outlines how to find common weaknesses in these systems. Real world examples and case studies are included. The talk concludes by illustrating possible defense strategies.

"The great Zamboni" has been in the security industry for over 6 years, most recently working at a Fortune 500 company. His work has covered many areas including penetration testing, assessing the security of systems and engineering computer security systems. Recently his job has focused on integrating physical and logical security systems. Outside of work Zamboni is a founding member of Miskatonic Research Labs, a non-profit security research group located in Northeastern Ohio. Some of his many interests include penetration testing techniques, wireless security, lock picking and the convergence of physical and computer security. He is also a core member of the Notacon planning committee.

The Unveiling of My Next Big Project
Philip R. Zimmermann, Creator, Pretty Good Privacy

Philip R. Zimmermann is the creator of Pretty Good Privacy. For that, he was the target of a three-year criminal investigation, because the government held that US export restrictions for cryptographic software were violated when PGP spread all around the world following its 1991 publication as freeware. Despite the lack of funding, the lack of any paid staff, the lack of a company to stand behind it, and despite government persecution, PGP nonetheless became the most widely used email encryption software in the world.

TUNE IN

DC TV

Staying at the Alexis Park? Want to see the talks but don't want to leave your room? Tune in to DEFCON TV!

Channels 22, 25, 27, 28, 29 & 30

IMAGE BY ASTROFY

DC RADIO

DefCon Radio is in it's 5th year this 2005.

For the last 4 years we have been working toward making the con more enjoyable through a DJ & Listener controlled radio station. This year will be the third year with that system.

The system broadcasts Vorbis OGG files through a custom ices & mysql combination to provide a somewhat scheduled but live interactive radio station.

When at the con: listen on 93.7fm @ the Alexis Park...

Updates on speakers and events every half an hour Interviews and news starting every hour

http://defcon.dmzs.com for updated information

BLACK & WHITE BALL

SATURDAY • JULY 31
2100 - 0400 • APOLLO

DJ	STYLE
wintamute/pmt munich	Electronic
DJ Casey	psytrance
Catharsis (EGR Records)	Hard Techno / Industrial
Miss DJ Jackalope	Dirty Drum and Bass
Regenerator	EBM
Shatter	Industrial
Krisz Klink	Psytrance

Come in Style: Rubber, Leather, Vinyl, Fetish Glam,
Kinky, Drag, Cyber Erotic, Uniforms, Victorian, Tuxedo, Costumes...
absolutely No Jeans or Street Clothes! No exceptions!!!

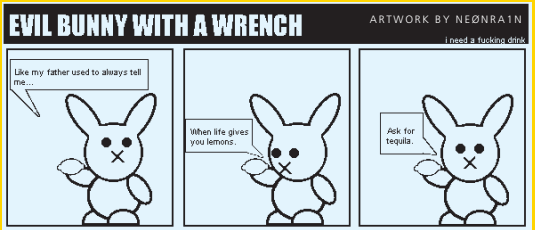
ORGANIZED BY BINK...BUY THE MAN A BEER

DAY 1 FRIDAY JULY 29	TRACK ONE PARTHENON	TRACK TWO TENT	TRACK THREE APOLLO
10:00 - 10:50	Recapturing the Revolutionary Heart of Hacking Richard Thieme	The Unveiling of My Next Big Project Philip R. Zimmermann	Hacking Nmap Fyodor
11:00 - 11:50	Mudge	End-to-End Voice Encryption over GSM Wesley Tanner & Nick Lane-Smith	On the Current State of Remote Active OS Fingerprinting Ofir Arkin
12:00 - 12:50	The Internet's March of Folly Paul Vixie	Routing in the Dark: Ian Clarke & Oskar Sandberg	Introducing Unicornscan Robert E. Lee & Jack C. Louis
13:00 - 13:50	Suicidal Linux Bruce Potter	Lost in Translation Christian Grothoff	ATM Network Vulnerabilities Robert Morris
14:00 - 14:20	CISO Q&A w/Dark Tangent Panel	Auto-adapting Stealth Communication Channels Daniel Burroughs	Credit Cards Robert "hackajar" Imhoff-Dousharm
14:30 - 14:50		The Next Generation of Cryptanalytic Hardware David Hulton	
15:00 - 15:20	No Women Allowed? Thomas J. Holt	The NMRC Warez 2005 Extravaganza Simple Nomad & the NMRC Collective	Hacking Google AdWords StankDawg
15:30 - 15:50	Social Engineering Do's & Don'ts Beth Louis (Phen)		
16:00 - 16:20	The Six Year Old Hacker Kevin McCarthy	Shmoo-Fu: Hacker Goo, Goofs, and Gear with the Shmoo Bruce Potter, Beetle, CowboyM, Dan Moniz, Rodney Thayer, 3ricj, Pablos	Passive Host Auditing jives
16:30 - 16:50	Development of An Undergrad Security Program Daniel Burroughs		Bypassing Authenticated Wireless Networks Pierce, Edwards & Lineberry
17:00 - 17:20	Whiz Kids or Juvenile Delinquents Amanda Dean		Mosquito Wes Brown & Scott Dunlop
17:30 - 17:50	The Power to Map Kristofer Erickson		
18:00 - 18:50	Hackers and the Media Patty L. Walsh	DC Groups Panel	Hacking Windows CE San
19:00 - 19:50	Causing the Law Mark Pauline	Death of a Thousand cuts Johnny Long	Your Defense is Offensive hellNbak
20:00 - 20:50	Assymetric Digital Warfare Roberto Preatoni & Fabio Ghioni	Hacking in a Foreign Language Kenneth Geers	
21:00 - 22:50	The Internet's March of Folly Paul Vixie	Black Ops 2005 Dan Kaminsky	TCP/IP Drinking Game hosted by Mudge

MOVIE CHANNEL

BROUGHT TO YOU BY DC801

	THURSDAY	FRIDAY	SATURDAY	SUNDAY
00:00		Primer	No Maps for These Territories	23
03:00		Brazil	The Day the Earth Stood Still	THX 1138
06:00		Pi	Blade Runner	The Fifth Element
09:00		Run Lola Run	Office Space	Enemy of the State
12:00		New Rose Hotel	Takedown	Fear and Loathing in Las Vegas
15:00	Oceans 11	Minority Report	I, Robot	Real Genius
18:00	Equilibrium	Ghost in the Shell	Ghost in the Shell 2	Pump Up the Volume
21:00	Wargames	Sneakers	Johnny Mnemonic	Hackers



HTTP://WWW.LIVEJOURNAL.COM/USERS/EVILBUNNYWRENCH/

DAY 2 SATURDAY JULY 30	TRACK ONE PARTHENON	TRACK TWO TENT	TRACK THREE APOLLO
10:00 - 10:50	Physical Security Bypass Techniques Mark Weber Tobias & Matt Fiddler	The Hacker's Guide to Search and Arrest Steve Dunker	Bacon Heman Gips
11:00 - 12:50	Introduction to Lockpicking and Physical Security Deviant Ollam	Ask EFF Newitz, Seltzer, Bankston, Opsahl, Schoen	Attacking Web Services Alex Stamos & Scott Stender
13:00 - 13:50	Intro to High Security Locks and Safes Michael Glasser & Deviant Ollam	Meet the Fed Jim Christy & Various other Feds	Automation - Deus ex Machina or Rube Goldberg Machine? Sensepost
14:00 - 14:50	A Safecracking Double Feature Leonard Gallion	The Information Security Industry David Cowan	
15:00 - 15:50	Attacking Biometric Access Control Systems Zamboni	Dr. Linton Wells Assistant Secretary of Defense for Networks and Information Integration	Pen-testing the Backbone Raven
16:00 - 16:50	Old Skewl Hacking - InfraRed Major Malfunction	Legal and Ethical Aspects of WarDriving Shuchman, Thornton, Hale II	Trust Transience: Post Intrusion SSH Hijacking Metalstorm
17:00 - 17:50	Building WarDriving Hardware Workshop Matthew L. Shuchman "Pilgrim"	Trends in Licensing of Security Tools Chuck Willis	Countering Denial of Information Attacks Greg Conti
18:00 - 18:50	Sketchtools Matt Cottam	Licensing Agreements 101 Jim "FalconRed" Rennie	The Dark Side of Winsock Jonathan Levin
19:00 - 19:50	Be Your Own Telephone Company...With Asterisk Strom Carlson & Black Ratchet	The Revolution Will Not Be Copyrighted Elizabeth Stark & Fred Benenson	Google Hacking for Penetration Testers Johhny Long
20:00 - 20:50		Top Ten Legal Issues in Computer Security Jennifer Granick	A New Hybrid Approach for Infrastructure Discovery, Monitoring and Control Ofir Arkin
21:00	Movie Night until 100 Hosted by the DarkTangent	Hacker Jeopardy	Black & White Ball until 0400

NOTEWORTHY

THE FIFTH ANNUAL DEFCON BAND OF RENEGADES SKYDIVE

The fifth annual very unofficial DefCon Skydive is scheduled for DefCon 13.

HTTP://WWW.DCJUMP.COM/

PREDEFCON SUMMIT

The Las Vegas, NV DefCon group, dc702, is proud to announce the pre-DefCon Summit!

What is it? TheSummit is a fund raiser for the EFF, a nonprofit group of passionate people - lawyers, technologists, volunteers, and visionaries - working to protect your digital rights.
ALL TICKET SALES GO DIRECTLY TO EFF

DETAILS
WHERE: Ice House - Las Vegas, NV
WHEN: Thursday July 28, 2005, 21:00 - 00:00
HOW MUCH: Tickets $30 pre-sale $40 @ door
All Ages Event!

WWW.DC702SUMMIT.ORG

RUMORZZZ

converge
The Turd in the Punchbowl
Join Date: Oct 2001
Location: slightly south of north
Posts: 1,691

Rumor has it, DT has taken the gunnery seat and will be personally accepting or denying every packet that touches defcon.org until the 1st of August. Be warned.

10 THINGS DEFCON HAS DONE FOR ME

SUBMITTED BY NIHIL

10. Made me hate Vegas
9. Introduced me to a bunch of great people
8. Given me something I can say I have done consistently for a decade
7. Taught me that drinking non-stop for 18 hours is a learned skill
6. Create the excuse needed to see those great friends once a year
5. Made me love Vegas
4. Paved the way to my current job (working for Black Hat)
3. Provided infamy by having my ex-girl friend (aka Bad Kitty) become Vinyl Vanna
2. Proven I never, ever want to share a room with one of the cDc again
1. Got me fired from Microsoft!

SLOGAN CONTEST WINNERS

1. Defcon: Putting the 13 in 31337 - panic
2. These aren\'t the geeks you\'re looking for. - Jack
3. def•con (dehf-cahn) n. 1.A tactical diversion by hackers to distract a large group of feds for a weekend. - Adrenaline

DAY 3 SUNDAY JULY 31	TRACK ONE PARTHENON	TRACK TWO TENT	TRACK THREE APOLLO
11:00 - 11:50	DIRA Alexey Smirnov & Tzi-cker Chiueh	Meme Mining for Fun and Profit Broward Horne	Forensic Data Acquisition Tools RS
12:00 - 12:50	Introducing the Bastille Hardening Assessment Tool Jay Beale	Hacking the Mind (Influence and NLP) Mystic	Visual Security Event Analysis Raffael Marty
13:00 - 13:50	The Insecure Workstation II `bob reloaded` Deral Heiland	Doing Not-For-Profit Tech Krembs, Farr, Tan, Cunningham, Granick, Schuyler, Wright & William Knowles & other select members of the Foundation Board.	Surgical Recovery from Kernel-Level Rootkit Installations Julian Grizzard
14:00 - 14:50	A Linguistic Platform for Threat Development Ben Kurtz	Analysis of Identity Creation Detection Schemes post-9/11 Cerebus	GeoIP Blocking Tony Howlett
15:00 - 15:50	"Shadow Walker" — Raising The Bar For Rootkit Detection Sherri Sparks & Jamie Butler	Why Tech Documentaries are Impossible (And why we have to do them anyway.) Jason Scott	Steve Dugan
16:00 - 16:50	Awards Ceremonies Hosted by the DarkTangent		

AFTER THE CON

Missed the last 12 DEFCONs? No phear! Revisit the past and relive the content with streaming audio and video. There are well over 750 live realmedia links. We expect you to be fully caught up before DC 14. To meet your privacy needs the main DEFCON website, which contains powerpoints and tools from previous talks, is now available via https.

http://www.defcon.org/html/links/defcon-media-archives.html or https://defcon.org/html/links/defcon-media-archives.html

Keep in touch with your local scene! There are DEFCON Groups all around the world, if there isn't one in your neck of the woods, learn how to start one. Like DEFCON the groups are a mix of security professionals and security enthusiasts. Technical projects, technical presentations, DEFCON contests, and other events are planned and executed by DC Groups.

http://www.defcon.org/html/defcon-groups/dc-groups-index.html

Even if you live in an isolated tundra, you can still participate in the DEFCON community long after the memories of the searing Vegas sun are gone. The DEFCON forums discuss technology, contests, events, as well as local DEFCON Groups meetings. A word to the wise—read the rules before posting. **http://forum.defcon.org/ or https://forum.defcon.org.**

After years of unsuccessfully attempting to gather the thousands of pictures taken at DEFCON the fine folks at DefconPics.org stepped up to the plate. In 2001 they took on the challenge of keeping track of every photo gallery in the universe that contains DEFCON related pics. Be advised, it is very likely that many of the pictures are *not* safe for work.

http://defconpics.org/

defcon 13 vendors

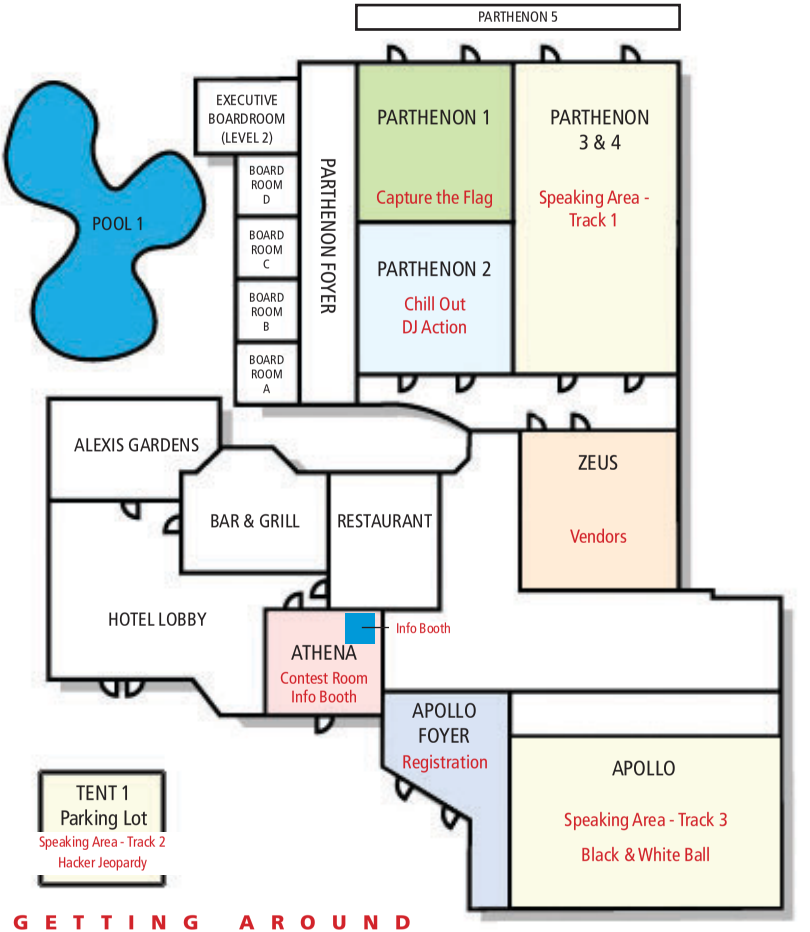
- Blacklisted 411
- Breakpoint Books
- CultureJunkie
- Electronic Frontier Foundation
- Irvine Underground
- Ninja Gear
- Overdose
- Rainbow
- Rootcompromise
- Shadowvex
- Sound of Knowledge
- Tim Huyn
- tommEE Pickles
- UNIX Surplus
- University of Advancing Technology
- WarDriving World

Vendors are located in Zeus. Vendor area is open from 1000 - 2000

Image courtesy of Rootcompromise.

DEFCON Looking for DEFCON Swag? Visit the Jinx booth in the Vendor Area and find T-shirts, shot glasses, mugs, bags, zippo lighters, hoodies, baseball hats, beanies, jackets, long sleeve shirts, camp shirts, laptop sleeves and more.

All official DEFCON merchandise have the DEFCON logo on them.



GETTING AROUND

Black & White Ball: Apollo
Capture the Flag: Parthenon 1
Contest Area: Athena
Dunk Tank: By Pool 2,
in front of the Gazebo
Info Booth: Athena
Hacker Jeopardy: Tent
Movie Night: Parthenon 3 & 4
TCP/IP Drinking: Parthenon 3 & 4
Vendors: Zeus

Speaking Track 1: Parthenon 3 & 4
Speaking Track 2: Tent
Speaking Track 3: Apollo

Lost your way? Go to the DC Info Booth located in the Athena.

THANKS TO THOSE WHO MADE DEFCON THIRTEEN POSSIBLE.

I want to personally thank everyone that has some together to make this con happen.
Because DEF CON is not a commercial enterprise in the sense that we can't afford to pay everyone who helps
(If we charged $250 a person, then it might be possible), it is in the hands of dedicated volunteers who make things happen.
This page is for them.

The Speakers, in Alpha Order: Ofir Arkin, Jay Beale, Wes Brown & Scott Dunlop, Daniel Burroughs, Strom Carlson & Black Ratchet, Cerebus, Ian Clarke & Oskar Sandberg, Greg Conti, Matt Cottam, David Cowan, Scott Blake & Pamela Fusco & Ken Pfiel & Justin Somaini & Andre Gold & David Mortman, Amanda Dean, Deviant Ollam, Steve Dunker Esq, Kristofer Erickson, Fyodor, Leonard Gallion, Kenneth Geers, Hernan Gips, Michael Glasser & Deviant Ollam, Paul Graham, Jennifer Granick, Julian Grizzard, Christian Grothoff, Deral Heiland, hellNbak, Thomas Jolt, Broward Horne, Tony Howlett, David Hulton, Robert "hackajar" Imhoff-Dousharm, Dan "Effugas" Kaminsky, jives, Jesse Krembs & Nick Farr & Emerson Tan & Frazier Cunningham & Jennifer Granick & James Schuyler & Christian Wright & William Knowles, Ben Kurtz, Robert E. Lee & Jack C. Louis, Jonathan Levin, Johnny Long, Beth "Phen" Louis, Kevin McCarthy, Major Malfunction, Raffael Marty, Jim Christy & various MIB, Metalstorm, Robert Morris Sr., Mystic, Annalee Newitz & Wendy Seltzer & Kevin Bankston & Kurt Opsahl & Seth Schoen, Mark Pauline, Dean Pierce & Brandon Edwards & Anthony Lineberry, Bruce Potter & Beetle & CowboyM & Dan Moniz & Rodney Thayer & 3ricj & Pablos, Roberto Preatoni (Sys64738) & Fabio Ghioni, Raven, Jim „FalconRed‰ Rennie, San, Jason Scott, Roelof Temmingh & Haroon Meer & Charl van der Walt, RS, Matthew „Pilgrim‰ Shuchman & Frank Thornton & Robert V. Hale II, Simple Nomad & HellNBak & erita & Weasel & jrandom & MadHat, Sherri Sparks & Jamie Butler, Alexey Smirnov & Tzi-cker Chiueh, Alex Stamos & Scott Stender, StankDawg, Elizabeth Stark & Fred Benenson, Richard Thieme, Mark Weber Tobias & Matt Fiddler, Patty "Muckraker" Walsh, Wesley Tanner & Nick Lane-Smith, Paul Vixie, Chuck Willis, Zamboni, Philip R. Zimmermann.

The Staff: Black Beetle, Zac, Dead Addict, Lockheed, Major Malfunction, Noid, Russ, Roamer, Techno Weenie, Priest, Cat, Q, Charel, Gonzo, Agent X, Nico, Heather, Videoman, Bink, Pyro, ETA, The Proctor, Zziks, Nulltone, Pappy, Cal, Wiseacre, Greg, OctalPussy, Noise, Quagmire Joe, Squeak, Flea, MikeyP, Cyber, Captain Jim, Rahael, Ben, KK, Nihl, D.Fi, SkrooU, Queeg, Quiet, Grifter, AlxR, Ted, Tyler, Sarge, CRC, Froggy, Connor, Cyber Junkie, Nobody, Teklork, B-Side, JDoll, Che, Freshm, TriggerJenn, Rescue, Dedhed, Kruger, CloneLoader, AJames, GodMinusOne, Justabill, Chosen 1, Pescador, Kevin E, Derek, Amish, Code 24, Riverside, Sn8keByte, FoTM, CYMike, Spahkle, Montell, Arclight, Kampf, Psylon, NFarr, Humperdink, CHS, Magic Tao, Koz, Xinc, Carric, Stephen Rossi, Dirk Sell, Jen M

The DJs: wintamute & pmt munich, DJ Casey, Catharsis, Ms. DJ Jackalope, Regenerator, Shatter, Krisz Klink.

Contest Organizers: CTF: the anonymous team behind kenshoto. Coffee Wars: Shrdlu, Alice, Madhat, Foofus. Hacker Jeopardy: Winn Schwartau & Nulltone. Lockpicking contest: KaiGoth, Freaky and Varjeal. Robot Warez: kallahar, jayandrews. Scavanger Hunt: tierra. Cannonball Run: tommEE. WarDriving Contest: Roamer, TheWad, Wiseacre, AlxRogan, Medic, Thorn, Syn-Ack. Slogan Contest: Roamer, Russ. Wifi Shootout: Dave Moore, Stefan Morris, Derek Hubbard, Steven Stovall. TCP/IP Device Contest: t0zi3, DC480. Toxic BBQ: converge, highwizard, l0nd0. Defcon Pics: tpublic. DC Movie Channel: DC801. QueerCon: HighWizard, euro12.

Those who will be remembered: Branden "Ghent" Hancock and Josh "PacBell" Cohen.

DEFCON