LAS VEGAS 2004

DEFCON 12

DEFCON GROUPS

A year ago we started an experiment, the DC Groups. It was an idea we put out to the community, a simple seed we planted. That seed has grown into a small garden. We take no credit for the growth; the success and future of DC Groups will has always been in the hands of the participants. One year ago we had five groups and now we have nearly fifty groups in the US as well as nine international groups from Iran to Malyasia, and from India to Italy.

More impressive than mere numbers of groups are what the groups are doing. Presentations are given, often recorded and served on various web sites, knowledge is being shared, projects are being initiated.

The philosophy behind DC Groups is similar to the idea behind DEFCON itself—create a forum, with a place and a time for people to meet exchange ideas, educate each other, work on projects, and have fun. Curiosity and willingness to share what you do know, not knowledge is required. If you are armed with curiosity and persistence you will gain knowledge and expertise. Focusing on a different technical topic each month is encouraged and allows for deep knowledge transfers. If you have any upcoming events or projects or video that you've created, we invite you to email us about them.

"How do I get involved?" See if there is an existing DC Group for your area (DEFCON.ORG has a listing of current sites), and contact the organizer or visit the web site. If an existing group isn't currently meeting, renewed interest and enthusiasm might be the only thing keeping it from re-igniting. If there isn't a group for your area mail dcgroups@defcon.org for information on how to start one.

Starting a DC GROUP is simple—have a time, a place, and a contact person for information. Having a small group of friends who are technically minded is a great starting point—your consistent attendance will help build the momentum towards a successful group.

WELCOME TO DEFCON 12

Welcome to DEFCON! I have been writing these welcome notes from the beginning, and you would think I would tire of them. In fact, it is one of the last things I do before the program goes to press, and is kind of a relief. We work all year long to get DEFCON ready for you, and once this gets written it signifies we are in a sort of terminal mode. Almost all the plans are set in stone, the shirts ordered, the art printed, the speakers are locked in, and now the physical packing begins to get the stuff of the con to the con!

As I write this it is almost out of my hands. I have made all decisions I can to make the show a success. To counteract the capacity problems we had last minute last year I have made speaking space the #1 priority this year. To match the space improvements I have also spent more time on the speaker selection process. I am proud to say that we have over seventy five speakers covering a wide range of topics. I think it is an excellent line up this year! I hope your problem will be in picking which talks to miss, instead of which to see.

I have moved around the vendor area, the speaking areas, and the contest area to maximize seating. We have given the info booth and the contests a dedicated area to better allow people to play, and we will record more of the contests.

With DEFCON I have always tried to focus on the tech, the hacking, the legal aspects, and the privacy surrounding these issues. I want a party where all like minded geeks and innovators can chill out and swap ideas. I want people to make new friends, become inspired for a new project, or to challenge an old one. I don't profess to have the answer to all security problems or how to deal with an ever larger big brother. I do think I can bring people together to talk about it, though. Some problems are technical, and some social. We can do two things at a time.

As usual, please don't destroy the hotel. If you manage to light yourselves on fire please consider the Geek Dunk Tank as good place to extinguish yourself. We have lined up some worthy people to be dunked, including myself.

While I could type all day about the improvements to the network, the addition of a WaveSec network (www.wavesec.org), the addition of more contests, the launch of the new game show, "'leetest link", etc. I'll just leave you with a thought; The Con is what you make of it. Do not be afraid to introduce yourself to others, or to ask questions of the speakers. We have provided you with a canvas, it is now in your hands to fill in.

See you by the pool.
The Dark Tangent DEFCON

BOOKSIGNINGS • ZEUS

Joe Grand
Fri, 1200

Scott Fullam
Fri, 1500

Bruce Potter
Fri, 1700

Bev Harris
Fri, 1800

Roamer, Russ Rogers
& Frank Fulton
Sat, 1200

Jon Erickson
Sat, 1400

Richard Thieme
Sat, 1500

bunnie
Sun, 1200

books are available for purchase from BreakPoint Books

DC FILM FESTIVAL

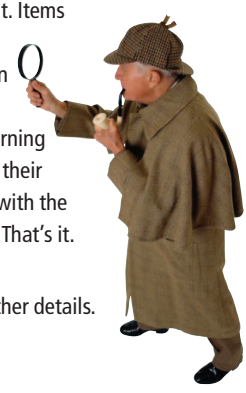
For years the scene has been creating homebrew documentaries, hacker media projects, and flash animations that mock and inform. Now some of those lucky people get rewarded and acknowledged for their efforts. DCFILMFESTIVAL.ORG contains rules for entries and will contain results. Watch DC TV for selected entries and winners—they will be placed in between movies on the DC movie channel. Enter next year and see your own creation on DC TV!

SCAVENGER HUNT

Welcome Back to the Defcon Scavenger Hunt. It's been a year and we're gearing up to once again catch Las Vegas with its pants down. The hunt will again be brought to you by the good folks of Utah, specifically slc2600 and Rootcompromise.org . We had so much fun last year we just knew we had to do it again.

The hunt works well when left undisturbed so we'll be sticking with the format that has worked in years past. For those of you that have competed in the hunt, you know what we mean. If you haven't yet had the pleasure of competing, you'll figure things out relatively quickly. It's a Scavenger Hunt Defcon style.

What exactly does that mean? Well, you'll be looking for items that range from Boots Full of Pudding to Candles shaped like Penises, and you'll have a blast doing it. Items are not limited to the physical of course, you may complete tasks to gain points for your team as well. You'll be given an Item List first thing Friday morning with a ridiculous amount of items and their corresponding point values. The team with the most points by Noon on Sunday, Wins. That's it.



Go to contest room and http://www.scavengerhunt.org for further details.

Leetest Link

What's this? Where's Hacker Jeopardy? What the hell is "The Leetest Link"?

The simplest explanation is...change. It's time to mix it up and make things better. Inject a little Hacker into another popular game show, and watch the sparks fly. We're stepping up the pace and adding twice as much game. Let me explain.

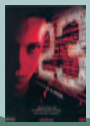
The game begins with 8 Players standing side by side and 2:30 minutes. Game play begins with the player furthest to the left of the audience. Time ticks down with players trying to amass as many points as they can in the smallest amount of time. Each time they answer a question correctly they get a chance to answer for a higher point value. The next player after a correct answer has the option to "bank" points so they cannot be lost due to an incorrect answer. At the end of each round the players vote to remove the one player of the game. This person leaves and gets nothing, they are not the Leetest Link. Ten seconds is removed from the clock and the Leetest Link from the previous round begins the next round. The game goes on like this until only two players remain. These two will complete a final round and at the end of said round their points will be doubled and added to all previously banked points. In the final round the two players will answer five questions each with the player with the most correct answers winning the game. This player is "The Leetest Link".

I hear you screaming already...What About Booze?!? Yes, "The Leetest Link" is a drinking game, get a question wrong or choose to pass, and you drink. In a time based game this is going to get interesting. You'll have to go as quickly as you can while trying to stay somewhat sober, good luck.

Richard Thieme, author of "Islands in the Clickstream: Reflections on Life in a Virtual World", speaker and writer extraordinaire will be hosting the game. If you've been coming to DEFCON and don't know Richard, it's time to leave the cave.

You can sign up to participate in the Contest Room, which is located in the Athena. See you there, and hopefully on stage.

24 hour movie cafe

	friday	saturday	sunday
0000 - 0030	The Matrix 	Matrix Reloaded 	Matrix Revolutions 
0100 - 0130			
0130 - 0200			
0200 - 0230			
0230 - 0300	Donnie Darko 	Dune 	Run Lola Run 
0300 - 0330			
0330 - 0400			
0400 - 0430			Fear & Loathing in Las Vegas 
0430 - 0500			
0500 - 0530	Scratch 	Blade Runner 	
0600 - 0630			Three Days of the Condor 
0630 - 0700			
0700 - 0730	Wargames 	Trainspotting 	
0730 - 0800			
0800 - 0830			Pi 
0830 - 0900			
0900 - 0930	23–Nichts ist so wie es scheint 	Real Genius 	
0930 - 1000			Cube 
1000 - 1030			
1030 - 1100			
1100 - 1130	Leon- The Professional 	Wonderful Days 	Boondock Saints 
1130 - 1200			
1200 - 1230			

1230 - 1300

1300 - 1330

1330 - 1400

1400 - 1430

1430 - 1500

1500 - 1530

1530 - 1600

1600 - 1630

1630 - 1700

1700 - 1730

1730 - 1800

1800 - 1830

1830 - 1900

1900 - 1930

1930 - 2000

2000 - 2030

2030 - 2100

2100 - 2130

2130 - 2200

2200 - 2230

2230 - 2300

2300 - 2330

thursday

Pump Up the Volume

The Fifth Element

Enemy of the State

X-files: Ghost in the Machine

Sneakers

Fight Club

Gattaca

The Shawshank Redemption

Kids in the Hall: Brain Candy

No Maps for These Territories

Office Space

Minority Report

The Day the Earth Stood Still

Equilibrium

Ocean's Eleven

The Bourne Identity

Johnny Mnemonic

Dark City

Hackers

ORGANIZED BY
DC801 AND
ROOTCOMPROMISE.ORG

key card
surekill

tshirt
haxor

tshirt
tdt

tshirt
Jesse

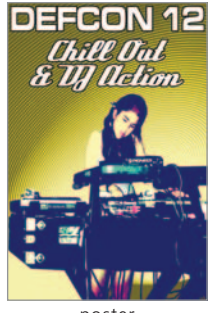
tshirt
bkbt

DC 12 Winner's Circle

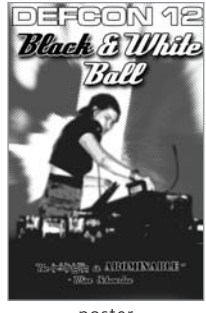
poster
bethar00

poster
doc

poster
insanity labs



poster
Jesse



poster
Jesse

FRONT COVER BY BX

SLOGANS

Winner: Belka
Find out what you don't know

2nd Place: ASTCell
HomeLAN Security

3rd Place: apacid
Your search for "Hackers of Mass Destruction" yielded no results.

wallpaper
[uranii]invid

poster
[uranii]invid

poster
flavah

DEFCON
PGP KEYSIGNING

SATURDAY • 1600 • ATHENA

Sign a PGP key today, starting with mine.

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. One

1. Make sure your PGP key is valid and the one you want to use. One people start signing it it is 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.

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. 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 that, 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

THE OFFICIAL DEFCON 12 WARDRIVING CONTEST

For the first time ever the DEFCON WarDriving contest will be divided into two parts. A "Main Drive" that will run for the entire three days and three "Mini-Games" that allow contestants that would like to participate but do not want to invest the entire Con in WarDriving. This page provides information on both facets of the contest.

Persons that sign up for the WarDriving contest are free to participate in all of the contests (Main Drive and all Three Mini Games) or any part. For instance, if you wanted to only participate in the "Treasure Hunt" Mini-Game, you are free to do so by registering for the contest. If, on the other hand, you wanted to participate in the Main Drive and "The Running Man" your registration affords you this opportunity.

DEF CON 12 CHECK-IN

Once you arrive at DEFCON, you will need to check in at the DEFCON 12 WarDriving contest sign in area located in the Def Con Contest Area.

DEFCON 12 WarDriving Contest: Main Drive

Sponsored by FAB-Corp
www.fab-corp.com

DEFCON 12 WARDRIVING CONTEST STAFF MEMBERS:
CHRIS, CONVERGE, THORN, ALXROGAN

TIMELINE OF EVENTS

Friday, July 30

- 10:00 AM CHECK-IN is open (CONTEST AREA in Athena)
- 12:00 PM CHECK-IN is closed

  NOTE: Anyone who has not checked in by that time will not be a participant in the DEFCON 12 WarDriving Contest.
- 1:00 PM The tournament will begin and upload capabilities will be enabled.
- 6:00 PM The upload server will be taken down for the night. Driving may continue but no logs will be processed until the server is back up.

Saturday, July 31

- Upload server will be made available as soon as WarDriving Contest Staff is able to confirm functionality. This is may not be a predictable time, so improvise; upload capabilities will be announced at the WarDriving table.
- 6:00 PM The upload server will be taken down for the night. Driving may continue but no logs will be processed until the server is back up.

Sunday, August 1

- Upload server will be made available as soon as WarDriving Contest Staff is able to confirm functionality. This is may not be a predictable time, so improvise; upload capabilities will be announced at the WarDriving table.
- Live scoring will not be done on Sunday. You will have to come to the Awards Ceremony to find out where you finished.
- 1:00 PM All logs must be completely uploaded according to dump specifications provided below to be included in contest results. No Exceptions, No Delays, No Malfunctions, etc...
- Contest winner announced at Awards Ceremony.

CHEATING: For those whom are intending to cheat... or even thinking about it... yeah you

WarDriver creativity is encouraged, but cheaters never prosper:

The DEFCON WarDriving Contest Staff will take precautions to prevent cheating.

Logs submitted by multiple persons to help a single wardriver advance in the contest is an activity strictly prohibited by the contest and will be treated as cheating.

If any member of a team is caught cheating the team will be disqualified without prejudice ("team" applies to mini games only as the main drive is individual).

Example of what is in store, more to be disclosed after the contest:

Several DSE's will be placed around Vegas. These are Access Points that will be turned off at the start of the contest. If the MAC for a DSE is in your data, you are disqualified.

CONDITIONS

DEFCON WarDriving Contest staff will conduct a pre-drive to establish a baseline. If a contestant's data significantly varies from the "baseline" the Def Con WarDriving contest staff will re-drive the area (same day). If the discrepancy still exists you will be disqualified.

DEFCON WarDi

FUNKSPIEL!

Suggested Equipment List For Playing In The DEFCON WarDriving Mini-Contests.

1) A WiFi enabled laptop or PDA.
2) GPS Receiver
3) Appropriate pigtails
4) Antenna cable(s)
5) An omni-directional antenna (suggested 5dBi to 8dBi)
6) A directional antenna (8dBi to 15dBi)
7) A compass
8) Maps (or mapping programs) of the Las Vegas area.

You are of course welcome to bring other equipment as you see fit. Just remember that some of the games may take place inside buildings. So choose appropriately. Do you really want to be dragging your 24dBi dish around inside a hotel?

FOX AND HOUND

Object: Be the first team to locate the "Fox."

Sponsored by NetStumbler.org (www.netstumbler.org)

and Michigan Wireless (www.michiganwireless.org)

Date/Time: Saturday, July 31, 18:00-21:00

- Time limit of 3 hours.
- Teams must be at least two people (driver & RF person/navigator) and limited to the total number of people who can safely sit in a single vehicle.
- No multiple vehicle teams.

12
riving Mini-Contests

RUNNING MAN

Object: Be the first to locate and id the "Running Man."

Sponosred by Blackthorn Systems
(www.blackthornsystems.com)

Date/Time: Saturday,July 31, 13:00-14:00

- Time limit of 1 hour.
- Limited to single players or two-person teams.
- Two person teams must work together, no splitting up allowed.
- Players should realize that this is DEFCON, and than means within 5 minutes of the contest's start approximately 492 spoofed RunningMan web servers will exist. The organizers cannot control this, so don't even bother to ask. Besides, it will add to the challenge. You don't want it to be TOO easy, did you?

TAG (YOU'RE IT!)

Object: The goal is to place a text file (yourname.txt) in a shared directory of a particular machine. 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.

Sponsored by FAB-Corp (www.fab-corp.com)

Date/Time: Friday July 30, 18:00-21:00

- Time limit of 3 hours.
- Limited to single players or two-person teams.
- The name and public PGP key of each player must be submitted before the start of the contest. (Two man teams may choose one team member's PGP key.)
- Two person teams must work together, no splitting up allowed.
- Once again, players should realize that this is DEFCON, and than means within 5 minutes of the contest's start approximately 8.6 million spoofed TAG servers will exist. The organizers cannot control this, so don't even bother to ask. Once again, it will add to the challenge.

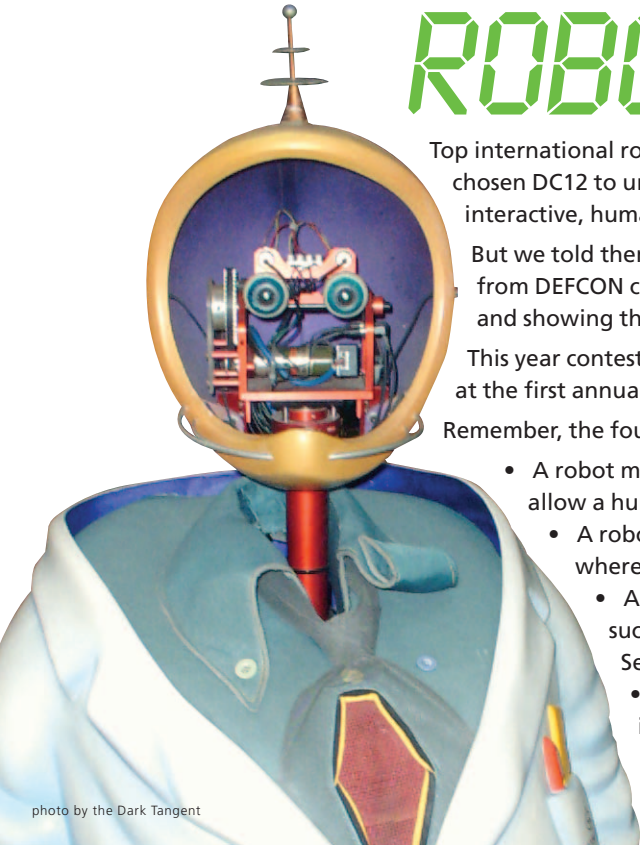


photo by the Dark Tangent

ROBOT WAREZ!

Top international robotics companies from around the globe have chosen DC12 to unleash their next generation of fully autonomous, interactive, humanoid robotic designs.

But we told them to go away as such a PR move would interfere from DEFCON contestants building their own homebrew robots and showing them off.

This year contestants will be showcasing their creations at the first annual Robot Warez competition.

Remember, the four laws of robotics are:

- A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- A robot must obey orders given it by human beings except where such orders would conflict with the First Law.
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.
- A robot must not humiliate Asimov by appearing in a substandard movie

For more information go to the contest area

ORGANIZED BY DC858

2nd Annual DEFCON Wifi Shootout Contest

2003 Grand Prize Winners:
team ASLRulz

Once again, wifi enthusiasts from around the globe will gather in Las Vegas, Nevada, July 30 - August 1, 2004, to pit their geeky skills against one another in the 2nd Annual Defcon Wifi Shootout Contest. The goal of the contest is simple: to achieve the greatest possible connect distance between two 802.11b stations through innovative engineering and antenna design. Held in conjunction with the annual Defcon conference, 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.

Those who wish to compete need to be familiar with all of the contest rules, found at http://www.wifi-shootout.com, and meet with Contest Staff at noon on Friday and Saturday, in the lobby of the Alexis Park. Don't be late!

ORGANIZED BY DAVE MOORE [XIP-E]
AND THE ASLRULZ TEAM

PRIZE SPONSORS

Assured Infosec http://www.ainfosec.com

JEFA Tech http://www.jefatech.com

Pasadena Networks, LLC
http://www.pasadena.net

Symantec http://www.symantec.com

Jinx Gamers, Geeks & Hackers
http://www.jinx.com

Wireless Fidelity Magazine
http://www.wirelessfidelitymag.com

Configuresoft
http://www.configuresoft.com

XCHANGE Magazine
http://www.xchangemag.com

Broadband Wireless Exchange Magazine
http://www.bbwexchange.com

O'Reilly Media http://www.oreilly.com

Netgear http://www.netgear.com

WIRED WHAT'S NEXT **Wired Magazine**
http://www.wired.com/wired/

IP APPLIANCE CONTEST

Have you finally cooked up your network aware Toaster? Does your coffee machine send SNMP packets to your server? Does your toothbrush send mail to you when you're running low on batteries?

If so, holy bloody hell, what are you DOING with your life? Or rather, you are now uber enough to enter the IP Appliance contest. Well, maybe next year, this year you can see what hardcore hardware geeks are doing with their time, and you can finally get the chance to hack someone's coffee maker.

prize sponsored by

PARALLAX INC

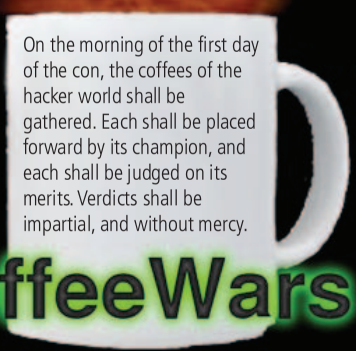
ORGANIZED BY DC858

Shall we play a game?
How about Global Thermonuclear Coffeewar?
Wouldn't you prefer a nice game of chess?
Later. Right now let's play
Global Thermonuclear CoffeeWar
Fine.

The date: 30 July 2004,
The time: 10:00AM
The place: Athena Room
DefCon 12
Alexis Park Hotel
Las Vegas, NV
USA
North America

FOUNDED BY ROB, ORGANIZED BY FOOFUS & THE COFFEEWARS CREW

Western Hemisphere
the Earth
the Solar System
the Universe
the Mind of God



For the fifth year, coffee-loving hackers will gather at DEFCON, bringing their finest coffee beans, and submitting them for judgment by a panel of enthusiastic and jumpy experts.

As always, judgments of the staff are final. Under the influence of enough coffee, these decisions may appear arbitrary, cruel, or irrational. This is why they call it a Coffee War: casualties are to be expected.

You like coffee? So do we. You think your coffee is good? Put it side by side with the best DEFCON has to offer, and find out.

Don't blow it, kiddo. Be there. With beans, and a good attitude.

The CoffeeWars staff awaits the chance to determine whether or not your coffee is the very finest in the whole world.

We have a (very) limited number of Coffee Wars V commemorative shirts, which will be made available on a first-come, first-served basis to entrants for the price of $15, at the time when you enter your coffee. Once they are gone, they are gone, and we can't do anything about that. This is the best (and only) known way to carry the glory of CoffeeWars V with you over the course of the coming year. If entrants do not purchase all the shirts, we will consider selling the remainder to interested non-entrants.

this photo from journal.codeslinger.com

GENERAL

The DEFCON 12 LockPick Contest will be held in three elimination rounds consisting of multiple 6-contestant heats over two days. Those people participating in other contest should let us know when registering and checking in. russrman is working on scheduling between contest to ensure that people aren't getting left out.

- There will be a maximum of 72 individual contestants for round one, dropping to 36 in round two, 12 for round three, and the top three individuals will compete in the final round to crown the winner.
- Individuals are responsible for providing their own equipment, no loaners will be available from the contest staff.
- This contest is free to all.
- There will be lock boards for people to practice on while the contest is not in process.
- We invite all experienced individuals to strut their stuff and help others.

CHECK-IN

- All 72 contestants will compete on Friday.
- Each individual must check in during the time specified in the Timeline of Events.
- Individuals may sign up for any open spots available or the alternate list during check-in as well.

RULES

- Only manual picks and tools will be allowed.
- Persons attempting to cheat will be eliminated from the contest.
- 72 individuals will compete in the first round, 6 at a time. The three fastest in each heat will move on to round two. Round two will consist of the 36 semi-finalists, 6 at a time as well. Again, the three fastest in each heat will continue to the finals. The remaining 12 will compete for the three top positions and a chance at the bonus lock.

SCORING

- This is an elimination event, and as such there is no scoring.
- To move on to the next round, simply pick the lock faster than those next to you!
- DEFCON Judges will determine who the winners of the heats are based on who completes the lock for the number of people that move forward in a heat (this will vary by heat). All judges decisions are final.

ORGANIZED BY DC 719

{ dc719.org }
HACK THE ROCKIES

LOCKPICK

PICK ARTISTRY

Those who can FEEL a pin drop

TIMELINE OF EVENTS

Friday, July 30th 2004
- Check-In
- Round 1

Saturday, July 31st 2004
- Round 2
- Round 3
- Finals

Sunday August 1st 2004
- Contest winner announced at Awards Ceremony.

this photo from acid.org

blast from the past

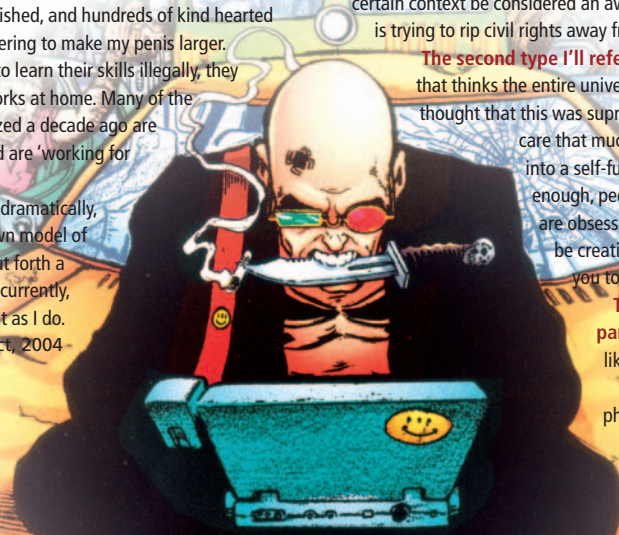
It's been about a decade since I wrote my rant on paranoia.

Since then our virtual landscape has changed quite a bit: the CDA come and and went, the DMCA came and stayed, russian mafia has become a player in cybercrime, Homeland Security was created, a cyberterrorist czar sat on the NSC, a foreign national has been imprisoned for writing decryption code, continual laws attempting to censor the internet to 'protect our children' have been passed and overturned, commercial interests have flourished and perished, and hundreds of kind hearted strangers email me every day offering to make my penis larger.

Hackers now no longer need to learn their skills illegally, they can cheaply create diverse networks at home. Many of the same hackers the media demonized a decade ago are active in securing cyberspace and are 'working for the man'.

While the world has changed dramatically, and is continuing to do so, my own model of paranoia has not - the model I put forth a decade ago is still one I describe currently, and I hope you still find value in it as I do.

—Dead Addict, 2004



FROM THE DEFCON 3 PROGRAM:

disclaimer: /nothing I say is true. Make this assumption before reading anything./

THERE ARE THREE TYPES OF PARANOIA.

The first type I'll refer to as 'impersonal'. This is the paranoia where one thinks that there are a lot of people out to get people, and could in certain context be considered an awareness of repression. "The government is trying to rip civil rights away from people" is an example.

The second type I'll refer to as 'irrational'. This is the paranoid that thinks the entire universe is plotting against /him/. I've always thought that this was supremely arrogant that the world would care that much. This, I've noticed, sometimes evolves into a self-fulfilling prophecy. If you rant long enough, people will start to talk about you. If you are obsessed with your impending doom, you may be creating it. The 'irrational' paranoia will lead you to be unhappy.

The third type is the 'rational' paranoia. This is the healthy kind. I also like to refer to this as 'being cautious'.

I'm going to direct this to hackers, phreakers, pirates, and any other breaking the law. You are breaking the law. The government, may, if they knew, try to 'get you'. It makes sense to prevent

this.

Many years ago, I was talking to Mind Rape on the phone, and he said (I'll paraphrase) "they're all out to get me, they're tapping my phone, they're watching my every move". He turned out to be correct, I thought he was wrong at the time, but being right was useless—he still got busted.

THINGS TO AVOID

Lets talk about things to avoid. Many of these are obvious.

Don't write things down. Little scraps of paper is probably the reason it takes the government 4 years to prosecute a person after they've been raided. But they do prosecute. Think of your output in terms of 'evidence'. Try to create as little of it as possible.

This includes a notebook! How to operate away from your house? Make a printout and burn it when your done. Realize that cops can trash just as easily as we can.

Gail Thackery and her ilk love our tradition of having a notebook that's rich in diverse information. Don't make their jobs any easier than you have to.

Use encryption. Encrypt everything. Make it easy (so you do it!), but don't compromise your security. Using all the encryption in the world doesn't help if you have a 'bust-me notebook'.

If people you know get busted, lay low for awhile. Be aware that the police probably have your number if he called you direct.

You shouldn't have to 'clean house', or go on an evidence destroying purge, because you shouldn't generate much evidence. System logs should be considered evidence as well.

If you have reason to believe you are going to be busted move your system elsewhere. Store your encrypted data someplace very safe (not where the system is located). When loaning out your computer, wipe (and government standard wipe!) your drive free of all data. Norton has a good wipe utility.

If you do most of your hacking from your own account, there's nothing I can say to make you smarter. Ditto with the home phone and phreaking.

Know the laws. Don't rely on hacker folklore. No matter how long your "really, I'm not a fed" BBS application is it won't protect you. It may in fact call attention to you, or confirm your illegal intents. Read the laws. Go to resources that are somewhat reliable. Don't expect your case to be a cause.

Know what crimes you're committing. Know the penalties. Know the jurisdiction (it could be FBI, SS, Local, State, or international authorities).

If you can, know the policies of your victims. For instance many people won't pirate Novell because of their Draconian tactics against BBS's who carry their warez. Many companies won't prosecute hackers because of their fear of loss of public trust and stockholder reactions. Many or most law enforcement investigations (concerning corporate hacks) start out because a company files a complaint. If they refuse to file complaints then they are much safer to penetrate.

Note that many corporate security officials have close ties with law enforcement. One day after a friendly informational interview with Microsoft Piracy investigator I received an email from a friend of Gail Thackery telling me to call her. This is a 'web' of enforcement, coordinated in many cases. Be aware of this, don't write off the person whose job it may be to find you. You don't ever want that attention, best if they never knew you were there.

There is a risk to everything we do in life. This is often part of the reason why we do it. Don't be scared, be informed and cautious—and hack, phreak, or pirate free from paranoia.

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.

Weaknesses in Satellite Television Protection Schemes, or "How I Learned to Love The Dish"

A

This is a beginning to intermediate level talk designed to give the participant a broad overview of satellite technology and where the holes are. I will not be teaching you how to steal service, but I will give you the background and information to understand how it could be done. Topics covered will include different programing you can receive, what kind of hardware you will need, and where to look for more info on the shadier side of things.

A has been involved in the local SLC "scene" for almost a decade, and is well read in many topics. He has many years of experience in most (legal) aspects of satellite and related technologies. A is always willing to help out those with a true interest in learning. He is currently working on a bachelor of science degree at Weber State University in Ogden, UT.

PDTP – The Peer Distributed Transfer Protocol

Tony Arcieri, PDTP.org

Despite decades of evolution, Internet file transfer is still plagued with problems to which formalized solutions are either inadequate or nonexistent. Lack of server-side bandwidth often renders high demand content inaccessible (which we affectionately refer to as the Slashdot effect). When the ability of a single server to provide content is exceeded, manual mirror selection is often utilized, providing an unnecessary and often problematic experience for end users. No formalized cryptographic mechanism exists for preventing tampering of files located on a particular server, and consequently malicious individuals have managed to place trojans in the releases of many high profile open source applications.

The Peer Distributed Transfer Protocol (PDTP) aims to solve all these problems. PDTP can either function with a network of servers providing content directly to clients, or can provide BitTorrent-like "download swarming" by forcing clients to participate in file transfers. PDTP includes built-in mechanisms to prevent file tampering through the use of the Digital Signature Standard, and is able to automatically verify that a given file has been signed by a DSA key with a complete x.509 certificate check to ensure a given certificate can be trusted. PDTP also provides a UDP-based decentralized search mechanism which, unlike current systems such as FastTrack, Gnutella, or FreeNet, does not consume undue bandwidth or system resources, all while removing legal liability for content indexing from the central services being utilized as entry points to the search system.

Tony Arcieri is a system administrator and programmer for the Pielke Research Group and Colorado Climate Center at Colorado State University. He has also contributed to a number of open source projects, including authoring the Ogg Vorbis plugin for XMMS, the cdcd and gdcd X11 CD player applications, and various contributions to other projects such as the Subversion version control system and the FreeBSD operating system.

Locking Down Apache

Jay Beale

Apache is the most popular webserver in use by most counts. While it doesn't have IIS's reputation as a worm target, it has still shown itself to be nowhere near invulnerable. Many Apache vulnerabilities can be countered proactively with hardening techniques—this talk will show you how to harden Apache to defeat exploits and worms that haven't yet been developed, or at least released.

Jay Beale is a security specialist focused on host lockdown and security audits. He is the Lead Developer of the Bastille project, which creates a hardening script for Linux, HP-UX, FreeBSD and Mac OS X, a member of the Honeynet Project, and the Linux technical lead in the Center for Internet Security, where he wrote the Unix host auditing tool in wide use today. Jay is a columnist with Information Security Magazine and has written for SecurityFocus, SecurityPortal and Incidents.org. Jay co-authored the Syngress international best-selling book on Snort, the new "Stealing the Network: How to Own a Continent" fictional book and serves as the series editor of the Syngress Open Source Security series, where he, HD Moore and Renaud

Deraison have just finished edits on a new book on Nessus. Jay makes his living as a security consultant through the MD-based firm Intelguardians, LLC.

Identification Evasion: Knowledge & Countermeasures

Adam Bresson, IT Manager

Everyday you're right to privacy is being compromised! From security cameras, to illegal searches, to unauthorized monitoring you are being watched. You must protect yourself...and your rights. Using Identification Evasion, you can immediately strengthen your protections. I'll discuss knowledge & countermeasures in the Computer and Real Worlds while presenting many great methods to turn the tables on surveillance. In addition to other in-depth demonstrations and examples, you'll see Identification Evasion in action as I present the video 'Night As Jason Biggs' (for the first time, unedited) where I applied these techniques in Las Vegas. You'll learn some things, enjoy the talk and be entertained!

Adam Bresson (adambresson.com) works during the day as an I.T. Manager for a Santa Monica Investment Banking firm. He also hosts a weekly Los Angeles open mic night, independently codes commercial web sites and challenges corrupt authority as often as possible. At DEFCON 8, he spoke on Palm Security. At DEFCON 9, he spoke on PHP, Data Mining & Web Security. At DEFCON 10, he spoke on Consumer Media Protections (CMP) generating considerable industry interest and press. At DEFCON 11, he spoke on Manyonymity: PHP Distributed Encryption releasing a GPL'ed suite of web application tools. Can you recognize him?

VICE - Catch the Hookers!

Jamie Butler, Director of Engineering, HBGary, LLC

Rootkits are the backbone of software penetrations. They provide stealth and consistent access to a computer system. Rootkits employ technology for covert ex-filtration of data, IDS evasion, and anti-forensics. Rootkit technology is now incorporated into the most deadly of threats, network worms. Serious security professionals must understand rootkit technology in detail. Commercial anti-virus technology is woefully inadequate at dealing with the threat. There is no magic security tool that will protect your system. Rootkits now employ specific methods to evade many security utilities, including host-based intrusion prevention systems (HIPS).

This talk focuses on specific rootkit threats and more importantly, how intrusion-prevention software can be designed to detect these threats. Illustrated threats include direct kernel object manipulation (DKOM), hooking, and runtime code patching. We will release a new version of our freeware tool, called 'VICE', that can detect many of these rootkit threats.

Jamie Butler is the Director of Engineering at HBGary specializing in rootkits and other subversive technologies. He is the co-author and a teacher of "Aspects of Offensive Root-kit Technologies." Prior to accepting the position at HBGary, he was a senior developer on the Windows Host Sensor at Enterasys Networks, Inc. He holds a MS in Computer Science from the University of Maryland, Baltimore County. 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.

How Do We Get The World To Use Message Security

Jon Callas, CTO & CSO, PGP

The time has come for people to start using email encryption extensively. There is enough threat from attackers as well as ignorant judges that email is not safe. SSL isn't good enough.

But how? How do we get people to do this? How do you get people whose VCRs blink 12:00 to use encryption? How do you get people to remember to encrypt?

This talk discusses both specific answers as well as open architectures to nudge people down the road of encrypting their email.

Jon Callas served as Chief Scientist at PGP Inc. and as CTO of the Network Security Division for Network Associates Technologies Inc. Mr. Callas served as Director of Software Engineering at Counterpane Internet Security Inc. and was a co-architect of Counterpane's Managed Security Monitoring system. Most recently, he was Senior

Systems Architect at Wave Systems Corporation. His career includes work at Digital Equipment Corporation, World Benders, and Apple Computer. He is the principal author of the Internet Engineering Task Force's (IETF's) OpenPGP standard and a writer and frequent lecturer on system security and intellectual property issues. Mr. Callas has a B.S. in Mathematics from the University of Maryland.

Program Semantics—Aware Intrusion Detection

Tzi-cker Chiueh, Professor, Stony Brook University/Rether Networks Inc.

One of the most dangerous cybersecurity threats is ``control hijacking" attacks, which hijack the control of a victim application, and executes arbitrary system calls assuming the identity of the victim program's effective user. These types of attacks are viperous because they do not require any special set-up and because production-mode programs with such vulnerabilities appear to be wide spread. System call monitoring has been touted as an effective defense against control hijacking attacks because it could prevent remote attackers from inflicting damage upon a victim system even if they can successfully compromise certain applications running on the system. However, the Achilles' heel of the system call monitoring approach is the construction of accurate system call behavior model that minimizes false positives and negatives.

This presentation describes the design, implementation, and evaluation of a Program semantics-Aware Intrusion Detection system called PAID, which automatically derives an application-specific system call behavior model from the application's source code, and checks the application's run-time system call pattern against this model to thwart any control hijacking attacks. The per-application behavior model is in the form of the sites and ordering of system calls made in the application, as well as its partial control flow. Experiments on a fully working PAID prototype show that PAID can indeed stop attacks that exploit non-standard security holes, such as format string attacks that modify function pointers, and that the run-time latency and throughput penalty of PAID are under 11.66% and 10.44%, respectively, for a set of production-mode network server applications including Apache, Sendmail, Ftp daemon, etc.

Dr. Tzi-cker Chiueh is currently an Associate Professor in Computer Science Department of Stony Brook University, and the Chief Scientist of Rether Networks Inc. He received his B.S. in Electrical Engineering from National Taiwan University, M.S. in Computer Science from Stanford University, and Ph.D. in Computer Science from University of California at Berkeley in 1984, 1988, and 1992, respectively. He received an NSF CAREER award in 1995. Dr. Chiueh's research interest is on computer security, network/storage QoS, and wireless networking. Dr. Chiueh's group developed the world's fastest array bound checking compiler that incurs less than 10% run-time overhead than programs without checking under Gcc, and built the world's fastest disk-based logging system, which accomplishes a single-sector disk write operation within 450 micro-seconds.

Freenet: Taming the World's Largest Tamagotchi

Ian Clarke

Since March 2000 the Freenet project has been the very embodiment of the "release early, release often" mantra, gaining invaluable experience of the unpredictable challenges encountered when deploying a P2P architecture on a large scale. This talk will discuss recent developments in the project including our "next generation" routing algorithm, and a sophisticated but elegant new load balancing mechanism called "adaptive rate limiting". Expect the talk to employ lots of real-world data to illustrate how theory translates to practice when looking after the world's largest Tamagotchi.

Ian Clarke is the architect and coordinator of The Freenet Project, and the Chief Executive Officer of Cematics Ltd, a company he founded to realize commercial applications for the Freenet technology. Ian is the co-founder and formerly the Chief Technology Officer 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. He is originally from County Meath, Ireland.

Network Attack Visualization

Greg Conti, Assistant Professor of Computer Science, US Military Academy

On even a moderately sized network, activity can easily reach the order of millions, perhaps billions, of packets. Hidden in this sea of data is malicious activity. Current network analysis and monitoring tools primarily use text and simple charting to present information. These methods, while effective in some circumstances, can overwhelm the analyst with too much, or the wrong type of, information. This situation is worsened by today's algorithmic intrusion detection systems, which, although generally effective, can overwhelm the analyst with unacceptably high false positive and false negative rates.

This talk explores the possibilities of visually presenting network traffic in a way that complements existing text-based analysis tools and intrusion detection systems. By graphically presenting information in the right way, we can tap into the high-bandwidth capability and visual recognition power of the human mind. Using the proper visualizations, previously masked anomalous activity can become readily apparent.

This talk will be of interest to those who wish to learn about information visualization as it applies to network security. It requires a basic understanding of the OSI model and packet encapsulation. Attendees will leave with an increased understanding of information visualization that they can apply to their own development projects and management of their networks.

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, interface design 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. He is conducting research into Denial of Information Attacks.

Electronic Civil Disobedience and the Republican National Convention

CrimethInc, Revolutionary Hacker Anarchist, CrimethInc Black Hat Hacker's Bloc

An introduction to the theory of hacktivism and the usage of hacking skills as a means of fighting for social justice by pressuring corporations and government to adopt progressive changes. Explores the history of electronic civil disobedience, tips on how to wage your own ECD campaigns, and how to participate in the upcoming actions to coincide with the protests against the Republican National Convention in late August.

CrimethInc is an Anarchist hacker revolutionary having led successful electronic civil disobedience campaigns against a variety of government and corporate targets. Experienced political activist, having helped organize dozens of large protests against the war in Iraq, global capitalism and neo-liberal free trade agreements. He is currently organizing a multi-pronged hacktivist campaign against the Republican National Convention to coincide with the massive demonstrations to take place in New York City. Specific history about the speaker is not available due to the nature of this project.

artwork by Mindshadow

IPv6 Primer

Gene Cronk (CISSP, NSA-IAM), North American IPv6 Task Force

The IPv6 Primer will encompass the basics of IPv6, including some of its roots, the transitioning mechanisms available, and some security

concerns early adopters should be aware of in several different environments. This presentation is meant for anyone who has heard about IPv6, but would like to know the basics of the protocol and its implementation.

Gene Cronk (CISSP, NSA-IAM), resides in Jacksonville, FL and is currently providing system administration services to an advertising and marketing firm.

He has 10 years of experience in electronics, system administration, networking and system security. Gene is best known for his work on the North American IPv6 Task Force, and his work onFu King Linux (an IPv6 enabled distribution of Linux), which includes security tools that can be run in IPv4 or IPv6 environments. He has also spoken on IPv6 and other topics at several venues.

When not totally absorbed by system security related issues, Gene can be found wardriving, actively participating as Vice President of the JaxLUG, and building a successful and dynamic 2600chapter, of which he is currently president.

Hacking the Media, and Avoiding Being Hacked By the Media

Dead Addict

Hackers have been demonized and romantisized in the media. Some hackers interactions with the media have caused their eventual incarseration, while others seem to pimp the media to promote their careers. Dead Addict will provide a framework for manipulating the media and avoid being the victim of the media. While this talk will be relavent to hackers, it is applicable to all that consume or are consumed by media. Dead Addict will also discuss methods to improve the quality of reporting and influence the media without appearing in it.

Considering himself a "great pirate" in the Buckminster Fuller sense of the term, Dead Addict has infiltrated some of the most powerful software publishers and financial institutions in the world.

Moving from hacker/poet to security systems analyst he is always trying get a handle on the 'big picture' while remaining a useful tool for multinational corporations. He has consistently been useful enough for them to allow him to be a full-time internal dissident.

Extensively studying global media influence as well as global activist politics has given him a healthy appreciation for appropriate levels of paranoia.

Dead Addict has been active organizer and speaker (at most Defcons) at Defcon for the last twelve years. He was a founding member of the now defunct criminal conspiracy calling themselves 'national security anarchists'. Actively appreciative of the statue of limitations, he has been involved in other 'underground' groups using various handles. This means nothing. Not believing in the concept of 'authority', he implores all that listen to him to evaluate his words according to their own value, not because of his BIO or 'who he is'.

The Open-Source Security Myth— and How to Make It A Reality

Michael Davis, DSCI

Open Source software is frequently described as more "secure" than closed source software for two reasons: the number of people available to correct a problem is potentially larger; and anyone can review the source code for vulnerabilities or malicious code. Unfortunately, the current state of design documentation does not support a cost-effective security review. In addition to compromising the confidence in the software, the lack of documentation also sets an unnecessarily high "bar" for new members to join an Open Source projects. This unintended consequence directly reduces the number of people available to correct vulnerabilities or otherwise improve the software. The presentation provides a rationale for creating development documentation and identifies available tools.

Michael Davis oversees the Security Engineering services provided by Dynamic Security Concepts, Incorporated (DSCI). During recent efforts to encourage his customers to use Open Source solutions; he oversaw the security review of a number of Open Source security tools. He possesses a broad security background and has been a featured speaker for select audiences on the subject of intrusion detection and evaluating security solutions in general.

DMCA, Then and Now

Dario D. Diaz

A look at the Digital Millenium Copyright Act (DMCA), what it was originally meant to do, what it's done, and how it's been used and abused. The highly misunderstood statute was hastily enacted and has been put to the test. While most in the hacker community might agree that the DMCA has been a failure, the actual legal results might actually provide some interesting insight. The lecture will involve an analysis of the statute, the legislative history, case law (both criminal and civil), and a perspective of the DMCA's future.

Shortly after joining the firm Diaz immersed himself in high profile litigation assisting partner Ralph Fernandez. In 1997 Fernandez and Diaz assumed the representation of three alleged Cuban skyjackers, Adel Regalado, Jose Bello Puente and Leonardo Reyes, on the night before testimony began in United States District Court. At the conclusion of trial the three defendants were acquitted of air piracy. Immediately the Immigration Service proceeded with detention and removal proceedings. In a highly publicized case in 1998 the Immigration Court ruled in favor of the three men granting them political asylum and withholding of removal. The government appealed to the Board of Immigration Appeal. A massive appellate process was undertaken. In October of 2002 the BIA affirmed the decision of the lower court. Fernandez and Diaz also assumed the representation of Jose Dionisio Suarez Esquival, implicated by the United States in the assassination of former Chilean Ambassador Orlando Letelier in Washington D.C. in 1976. During the process Suarez became entangled in the extradition proceedings of General Augusto Pinochet by the Kingdom of Spain and the ancillary investigation by the Republic of Chile. In August 15, 2001, Suarez was freed after nearly a decade of detention. Diaz walked Suarez Esquival out of jail. The photo grabbed headline news around the world. Diaz later directed the successful defense in State of Florida v. Noe Ramirez, at one time identified as the individual that tossed a boulder off the I-75 overpass in Bradenton, Florida, tragically killing a well known and respected University of Alabama professor.

artwork by Bean

In August of 2000, Diaz was asked to speak at DEFCON, the largest conference for computer security, cryptography and hacking held in the United States. His lecture dealt with the Digital Millennium Copyright Act (DMCA) and the legal aspects of the law. A Russian programmer and citizen, Dmitri Sklyarov, who was also a conference lecturer, was arrested by federal authorities for criminal charges stemming from the DMCA. In news stories the national media identified Diaz as the leading expert in the area. Diaz', trial practice involves civil, criminal, and family law cases. He has tried cases in criminal, personal injury, negligence, and select family law matters.

Tor: An Anonymizing Overlay Network for TCP

Roger Dingledine, The Free Haven Project

Tor (second-generation Onion Routing) is a distributed overlay network that anonymizes TCP-based applications like web browsing, secure shell, and instant messaging. We have a deployed network of 30 nodes in the US and Europe, and the code is released unencumbered as free software. Tor's rendezvous point design enables location-hidden services—users can run a standard webserver or other service without revealing its IP.

I'll give an overview of the Tor architecture, and talk about why you'd want to use it, what security it provides, and how user applications interface to it. I'll show a working Tor network, and invite the audience to connect to it and use it.

Roger Dingledine is a security and privacy researcher. While at MIT he developed Free Haven, one of the early peer-to-peer systems that emphasized resource management while retaining anonymity for its users. Currently he consults for the US Navy to design and develop systems for anonymity and traffic analysis resistance. Recent work includes anonymous publishing and communication systems, traffic analysis resistance, censorship resistance, attack resistance for decentralized networks, and reputation.

Far More Than You Ever Wanted To Tell— Hidden Data In Document Formats

Maximillian Dornseif

Applications usually put all kinds of information besides the ones which you intend to into saved documents. This can lead to embarrassing revelations. We will take a look into different types of application data and what can be hidden in there. This allows us to "scrub" our own documents to avoid unwanted information in there but also to look for information in documents which the authors didn't want to hand out. Go grasp the scope of the problem we will present a large scale study of hidden information in Documents on the Internet.

Maximillian Dornseif has studied laws and computer science at the University of Bonn, Germany where he wrote his PhD Thesis about the "Phenomenology of Cybercrime". He has been doing security consulting since the mid nineties. His clients included the industry but also government. At the moment he works on a third party founded research project about measurement of security and security breaches taking place at the Laboratory for Dependable Distributed Systems, RWTH Aachen University. He also oversees several other projects in the area of detection and documentation of security incidents. Dornseif has published in the legal and computer science fields on a wide range of topics.

Credit Card Networks Revisted: Penetration in Real-Time

Robert "hackajar" Imhoff-Dousharm, Credit Card Compliancy and Fraud Analyst

Jonathan "ripshy" Duncan, Systems Developer to demonstration

Credit card authorization is the core to all major businesses, both on and off the Internet. Yet an alarming number of businesses are not taking the right steps to insure that your credit cards are secure against fraud and theft. In bringing this to light (Credit Card Networks 101, DC 11), you were awed at the posibility, but were not provided with any real proof. This year we, that's you and I, will walk through the process of identifying credit card traffic on a network, deciphering packets and propagated rouge credit card data to a host comeputer. You will be provided access to a private Wi-Fi network. This networks will have credit card data streamming across it for you to sniff. With your help, we will discover information about credit cards packets, and how to design our own packet to be sent.

Want to partcipate?

Login to http://www.hackajar.com/credi

Read "What's in a credit card" section for background on credit cards and their supporting networks

Read "What you'll need" section, and have said items at conference

Sign-up for fake credit card account, you will use this to keep track of your progress and win prizes

NOTE: You will have opportunity to sign-up for account during demonstration

In the last 2 years, Robert "hackajar" Imhoff-Dousharm has worked for Shift4, a Credit Transaction Gateway. As an Analyst he insures best fraud practices, compliancy and security are met at all clients sites He has worked with government agency's during fraud investigations. He also works with new and potential clients to implement best practice in software design of credit card intigration software Robert has spoken at DefCon 11 (Credit Card Networks 101) about the potential risks currenly impeading on credit card networs. He will demonstrate those risks this year with "Credit Card Networks Revisted: Penetration in Real-Time".

Kryptos and the Cracking of the Cyrillic Projector Cipher

Elonka Dunin

In a courtyard at CIA Headquarters stands an encrypted sculpture called Kryptos. Its thousands of characters contain encoded messages, three of which have been solved. The fourth part, 97 or 98 characters at the very bottom, have withstood cryptanalysis for over a decade. The artist who created Kryptos, James Sanborn, has also created other encrypted sculptures such as the decade-old Cyrillic Projector, which was cracked last September by an international team led by Elonka

Dunin. This talk is intended for a general audience with beginning to intermediate cryptographic experience. Elonka will go over how the code was cracked, and the current state of knowledge about the Kryptos sculpture, its own encrypted messages, and its mysterious CIA surroundings.

Elonka Dunin is a professional game developer, working at Simutronics (play.net), a provider of massively multiplayer online games. Also an amateur cryptographer, Elonka led the international team that cracked the decade-old KGB Cyrillic Projector Code in September 2003.

Elonka was born in Los Angeles, studied Astronomy at UCLA, and then joined the United States Air Force, where she worked on the SR-71 and U-2 reconnaissance aircraft. Elonka is a world-traveler who speaks multiple languages, and has visited scores of countries around the world, and every continent (yes, including Antarctica). She has won awards for cracking various codes, such as when she cracked the PhreakNIC v3.0 Code, an up-until-Elonka unsolved puzzle created by se2600. Since September 11th, Elonka has also been helping out with the war on terrorism by teaching government agents about cryptography and what types of codes that Al Qaeda may be using. She is co-founder of the Kryptos Group, an online group of cryptographers and interested hobbyists trying to crack the last part of the code on the famous Kryptos sculpture at CIA Headquarters.

Hacking/Security Mac OSX Server aka Wussy Panther

Charles Edge aka krypted, Senior Systems Engineer, Three18

Panther Server, the highly touted new OS by Apple has some glaring security flaws, although Apple typically gets away easy because not a lot of people hack it. See what's being done against OSX Server and what can be done to guard against it.

During the talk, I will show exploits I've been working on since Panther was released and give honorable mention to the tools I've been using to help me out along the way.

Remember when BackOffice came out and there were a bunch of exploits against it? Well, imagine another server with web-based email, a full web development platform, SQL, and File Sharing over a proprietary protocol.

No Apple knowledge is required of the listener, only a working knowledge in UNIX.

Charles Edge has been setting up and maintaining hybrid networks for the entertainmentindustry (including the Osbournes) in Los Angeles for 5 years. This talk will focus on hardening OSX Server by showing its vulnerabilities.

MySQL Passwords— Password Strength and Cracking

D. EganSenior , Web Applications Developer, ICS MT

This talk will cover best practices for choosing MySQL passwords as well as the tools available to "crack" a MySQL password hash. It will NOT cover how to obtain a password hash, however. During the talk I will be introducing a new dictionary-based auditing tool, named "phpMyAudit". The tool is written in PHP and allows a user to run the application as a shell-based script, yet it also includes a web-based front end. This talk is primarily aimed at persons interested in choosing secure MySQL passwords, and persons who would like to "audit" an existing MySQL password hash.

D. Egan is a recent college graduate who has been a professional web-application developer for over 5 years. He currently works and lives in beautiful Missoula, Montana. This will be his 5th year attending Defcon, and his first Defcon speech.

Information Hiding in Executable Binaries

Rakan El-Khalil

Information Hiding techniques are much researched in the context of watermarking or fingerprinting images and sound files, mainly as a means of copyright protection and piracy prevention/detection. Those mediums offer a significant amount of redundancy, thus lending themselves to the implementation of robust IH systems. Executables however do not offer such amounts of redundancy, and have thus far proven to be a difficult and rarely used medium for steganographic and other IH purposes. The aim of this talk is to be an introduction to IH, with a thorough coverage of state of the art techniques for embedding into binaries. Hydan, a tool for performing such

embeddings in machine code, will be presented. In addition to typical IH uses [steganography, watermarking], the tool and techniques shown can be used in anti-reverse engineering, trusted application execution, frustrate some buffer overflow attacks, and as an engine for metamorphic viruses. An interesting effect of the tool is that the executable remains the same size before and after embedding, while of course remaining functionally equivalent.

Rakan El-Khalil is currently on sabbatical in France. He is a recent MS CS graduate from Columbia University. While he was there he worked on a variety of projects at the CS Research Lab, such as an IDS that uses machine-learned models to detect network threats, and a syscall based permission system on OpenBSD [predating systrace]. He was also responsible for the short-lived official KaZaA Linux client `kza'. Currently he is involved with The Bastard, a powerful linux disassembler, and has been researching steganography and information hiding in machine code.

"We Can Take It From Here"

FX, Phenoelit
Halvar Flake

Sick of watching other people working their magic and still wondering how to get 0day? Write your own! This session is about the state of mind for finding and exploiting bugs. From web applications to client-server systems and multi-tier platforms down to routers, switches and wrist watches - everything has bugs and everything can be exploited one way or another.

artwork by flavah

But of course, a state of mind alone doesn't get you 0day. Now you need to find a crack in the armor that you can pry open and drive your truck through.

The session will try to guide you through how to find a bug, how to combine several of them or how to circumvent things that would ruin your plan, starting from how to do educated guesses down to diff and patch review.

Don't be scared, have no phear. Found a bug but you have no idea what to do with it? A strange CPU, a never-seen-before platform or an unknown protocol should not prevent you from getting r00t anyway. This last part deals with guidelines on shell and non-shell codes, binary or not, and with handling complicated platforms.

The goal is that you walk out with your own 0day already developing in your mind.

FX of Phenoelit is the leader of the German Phenoelit group. His and the group's primary interests are in security implementations and implications of standards or less-known protocols, as shown on past DefCon conventions. FX has a fairly special relationship with shops like Cisco Systems and HP as well as SAP. Currently, he works as a Security Solution Consultant at n.runs GmbH.

Halvar Flake is Black Hat's resident reverse engineer. Originating in the fields of copy protection, he moved more and more towards network security after realizing the potential for reverse engineering as a tool for vulnerability analysis. He spends most of his screen time in a disassembler (or developing extensions for the disassembler), likes to read source code diff's with his breakfast and enjoys giving talks about his research interests. He drinks tea but does not smoke camels.

The First International Cyber War: Computer Networks as a Battleground in the Middle East and Beyond

Peter D. Feaver, Professor, Duke University
Kenneth Geers, Analyst, NCIS

This briefing addresses the world's first global Internet war: the cyber skirmishes associated with the Palestinian intifadah. What started out as a localized conflict spread to battles around the globe as forces sympathetic to either the Israelis or the Palestinians joined the fray. With the Middle East cyber war as a backdrop, this presentation will cover the ways in which people can try to affect the course of world history through coordinated action in cyberspace.

The authors first describe the globalized and asymmetric nature of modern warfare, the asymmetry of computer hacking, and the psychology of subcultures. They outline the legal issues surrounding

cyber warfare, from the perspective of a lone hacker to a massive government intelligence service, and discuss the problems inherent in cyber retaliation and in the prosecution of hackers.

On the technical side, this briefing discusses the targeting of Internet sites for attack, and the strategies used by hackers to bring them down or merely leverage them in more subtle ways to support their cause. The primary focus is the means used by cyber commanders to accomplish political and/or social goals, in particular the creation of Web portals through which their foot soldiers are able to unite and rain network packets down upon their enemies.

Finally, this briefing examines the difference between the perception and the reality of cyber attacks. We address the strategies that national governments are employing to combat the threat, the potential impact of cyber attacks on military operations, and the vexing problem of Denial of Service attacks, Web defacements, and free speech. The authors assess the threat and the limits of the more powerful weapons in the cyber arsenal, and consider who might be the biggest target of cyber attacks in the coming years.

Peter D. Feaver (Ph.D., Harvard, 1990) is Professor of Political Science and Public Policy at Duke University and Director of the Triangle Institute for Security Studies (TISS). Feaver is co-directing (with Bruce Jentleson) a major research project funded by the Carnegie Corporation, "Wielding American Power: Managing Interventions after September 11." Feaver is author most recently of "Armed Servants: Agency, Oversight, and Civil-Military Relations" (Harvard Press, 2003),and co-author, with Christopher Gelpi, of "Choosing Your Battles: American Civil-Military Relations and the Use of Force" (Princeton University Press, 2004). He is co-editor, with Richard H. Kohn, of "Soldiers and Civilians: The Civil-Military Gap and American National Security" (MIT Press, 2001); and author of "Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States" (Cornell University Press, 1992). He has published several other monographs and over thirty articles and book chapters on American foreign policy, nuclear proliferation, civil-military relations, information warfare, and U.S. national security. In 1993-94, Feaver served as Director for Defense Policy and Arms Control on the National Security Council at the White House where his responsibilities included counterproliferation policy, regional nuclear arms control, the national security strategy review, and other defense policy issues. He is a Lieutenant Commander in the U.S. Naval Reserve (IRR).

Kenneth Geers (M.A., University of Washington, 1997) is a Computer Investigations & Operations analyst with the Naval Criminal Investigative Service (NCIS). His career at the Department of Defense also includes work at the National Security Agency, the Defense Intelligence Agency, an SAIC nuclear arms control support team, the John F. Kennedy Assassination Review Board, and the U.S. embassy in Brussels, Belgium. He is an expert in French and Russian, who finished first in a class of seventy at the Defense Language Institute at the Presidio of Monterey. Mr. Geers is the author of training and testing software to prepare U.S. Army Major Commands for Russian strategic arms inspections, and he has designed multiple U.S. Army Space and Missile Defense Command websites devoted to arms control. These days, he spends his time analyzing computer and network logs of all types. In his free time, he plays chess and serves as a SANS mentor in the Washington D.C. area. Over the years, he has taken the opportunity to see the world, stopping long enough to wait tables in Luxembourg, harvest grapes in the Middle East, climb Mount Kilimanjaro, and set his alarm clock for 3 AM in a strict Trappist monastery.

Attacking Windows Mobile PDA's

Seth Fogie, VP, Airscanner

Microsoft's Pocket PC (AKA Windows Mobile) has remained relatively free of all the nasty attacks that have bombarded its PC based cousins. Does this mean this OS is any more secure or safe from attack? Ironically, this is as far from the truth as one can get.

Using reverse-engineering techniques, this presentation will demonstrate just how easy it is to gain full remote unauthorized access to a PPC device. In addition, we will also provide an example of a remote buffer overflow attack against the PDA and the tricks needed to place working code on the proverbial stack.

This talk will be technical. However, if you want to gain a better understanding of the ARM processor, hacking Pocket PC programs, or just want to see how buffer overflow attacks work on the PDA, you will not be disappointed.

Seth Fogie is the VP of Dallas-based Airscanner Corporation where he oversees the development of security software for the Window Mobile (Pocket PC) platform. He has co-authored four technical books on information security, including the top selling "Maximum Wireless Security" from SAMS, and the recently released "Security Warrior" from O'Reilly. Mr. Fogie frequently speaks at IT and security conferences, including Defcon (10 & 11), CSI, and Dallascon. In addition, Seth is acting Site Host for Security at Pearson Education's "InformIT.com" website where he writes articles and reviews/manages weekly information security related books and articles.

Old Tricks

Foofus

In September of 2003, a noted security consultant was terminated from his job over controversy surrounding a document that he co-authored. One key focus of the document was the risk associated with operating system monocultures. This idea was nothing new. In fact, in 1989, the following passages appeared in a book that spent over four months on the New York Times best seller list:

> "Just like genetic diversity, which prevents an epidemic from wiping out a whole species at once, diversity in software is a good thing."
>
> "A computer virus is specialized: a virus that works on an IBM PC cannot do anything to a Macintosh or a Unix computer. [snip] Diversity, then, works against viruses. If all the systems on the Arpanet ran Berkeley Unix, the virus would have disabled all fifty thousand of them. Instead, it infected only a couple thousand."
>
> — Stoll, Cliff. THE CUCKOO'S EGG, New York: Simon & Schuster Pocket Books, 1989. Pages 51 and 347.

The point of this citation is not to cast any disrespect on the authors of "CyberInsecurity: The Cost of Monopoly" (on the contrary, in fact). Rather, we wish merely to note that the risk of monocultures was identified at least fourteen years ago, and was widely published. Why fuss if someone repeats it?

Foofus.net wants in on this kind of action. In that spirit, we've looked high and low for a bunch of other old ideas so that we can breathe new life into them, and (in the famous words of a respected security research team), make "the theoretical practical," in an effort to tax the patience of those who would rather we kept our heads in the sand about ideas that are right there in the open, but inconvenient to demonstrate. Until now.

Come to this presentation, and savor some exquisite fun. We will demonstrate our tools and techniques, and we think you will find that they are interesting and useful. But not new. We promise that we have not invented a damn thing here; the basic concepts are 100% recycled, but we hope they will encourage people to get serious about areas where they've been coasting for too long.

The focus of the talk is Windows: tools will be presented for identifying potential trust relationships between disparate hosts, tinkering with friendly wireless interfaces, easy access to network shares without bothering to crack password hashes, and (if our luck holds) maybe even a little more. It'll be really fun, and stuff.

Foofus leads a team of security engineers at a midsize technology consulting firm in the midwest, where he has worked for the past seven years. He has spoken at a variety of events and conferences including Toorcon and LISA. His chief technical interest is software security, and in his spare time he enjoys playing guitar, cooking, and attending the symphony.

Introduction to Hardware Hacking

Scott Fullam

Interested in hardware hacking but were not sure where to start? This presentation is for you. I will show you how to get started with modifying equipment for fun and useful purposes. I will show you the best ways for opening the enclosures for electronic equipment without destroying it, how to identify electronic components, how to

solder together circuits, where to get parts, and will do a walk through of several hacks i have completed. the talk is intended for beginners, but all experience levels will get a kick out of it.

Scott Fullam is the author of the O'Reilly book "Hardware Hacking Projects for Geeks" published in February 2004.

Scott Fullam has been hacking hardware since he was 10 years old with his first RadioShack 100-in-1 electronic kit. He built an intruder alarm to keep his sister out of his room. Scott attended MIT earning Bachelors and Masters degrees in Electrical Engineering and Computer Science. While and undergraduate he built a shower detection system so that he could see if the community shower was in use to allow him to sleep in a few extra minutes in the morning if it was occupied. After graduating from MIT Scott designed children's toys and built close to 50 prototypes in 2 years. He then went to work at Apple Computer in the Advanced Technology Group designing digital still cameras. In 1995, Fullam co-founded PocketScience, which develops revolutionary mobile e-mail communications products and services. As the Chief Technology Officer (CTO), Fullam personally developed all of the algorithms for the company's products. He also led the team that developed PocketScience's products and reference hardware. Scott now works as an independent consultant assisting consumer electronic companies design high quality products and manufacture them in the Far East. Scott holds 15 US patents. Never satisfied with how the consumer electronics products he own work, he often takes them apart and enhances their capabilities.

This Space Intentionally Left Blank

Geoffrey
Mark Farver

"This Space Intentionally Left Blank" covers work done to safely allow the transfer of unclassified data onto a sensitive (read highly classified) network for comingling with other data collects andsubsequent analysis. We devised a system using COTS (Commercial Off The Shelf) hardware, Open Source applications and a couple of custom programs to accomplish these ends. The main requirement was to ensure a one way flow of data from the antenna farm into the analysis network with no data drift back. The presentation will discuss the technical details of how this was managed.

Geoffrey has been a facility and network security officer and ComSec Manager in the Intelligence Community for fourteen years. His duties include shoring up network security at both contractor and government facilities. He is also available for childrens' parties.

Mark Farver has served 5 years as trampled network engineer and code monkey. He has spent the past two years as network administrator and ComSec manager for sensitive networks. He knows little of value and sometimes gets cranky without a nap.

What Do You Mean, Privacy?

Sarah Gordon

Privacy doesnt mean the same thing to everyone... Since you're interacting in a global space, you need to understand what people outside your immediate frame of reference are thinking when they talk about privacy—because what they think will influence ttheir expectations and their actions. This talk will give you the opportunity to examine some other views of privacy, explore your own thinking, and compare it with others—both from the global information security community and the audience. Finally, we'll look at how well those thoughts match up with behaviors related to various aspects of what we call "privacy".

Sarah Gordon has spoken at DEFCON on topics from the security of PGP, women of #hack, and the impact of legislation on virus writing, and done lots of security related stuff for lots of different groups.

Advanced Hardware Hacking: Designs and Attacks of Secure Hardware

Joe Grand, aka Kingpin, Electrical Engineer, Grand Idea Studio

artwork by bx

This presentation looks at advanced hardware hacking and reverse engineering techniques. We'll look at the steps taken by designers to incorporate security into their hardware products and then examine ways to attack them. Learning from history is

important, so successful hardware hacks against security products will be discussed and copious references to other existing material will be provided.

Joe Grand (also known as Kingpin) is an electrical engineer at Grand Idea Studio, Inc., a product development and intellectual property licensing firm. He is a former member of the legendary hacker collective L0pht Heavy Industries (yes, which turned into @stake, but don't ask him about that) and specializes in embedded system design, computer security research, and inventing new concepts and technologies.

Oh, Joe is also the author of the Syngress book "Hardware Hacking: Have Fun While Voiding Your Warranty" published in January 2004 and contributor to a bunch of other books.

Tools for Censorship Resistance

Rachel Greenstadt, Harvard University

What censorship resistance technique is right for me? (And should my Chinese dissident friends use the same one?)

Nearly everyone in the world is affected by censorship to some degree. Whether from annoying corporate firewalls, nervous ISPs, or oppressive governments, the result is often the same; individuals and organizations are unable to obtain information they want, say the things they'd like, or communicate with others. A number of technologies are helpful in circumventing these restrictions, including covert channels, steganography, and peer-to-peer systems.

This presentation will survey the field of censorship resistance and discuss the maturity and promise of various techniques, as well as their promise and limitations from a theoretical perspective. I will present a range of capabilities and threat models and discuss which approach is best suited to each situation.

Rachel Greenstadt is a researcher at Harvard University and a DHS fellow. She studies how information is leaked, collected, and controlled. She has done research on privacy, steganography, covert channels, and peer-to-peer security. Rachel is a contributor to the forthcoming book, The Economics of Information Security. She attends small, academic conferences compulsively, takes ballet classes, and reads science fiction in her spare time.

Project Prometheus

Grifter
Russ Rogers, CEO & CTO, Security Horizon
Tierra

The goal of Prometheus is to create an Open Source project that takes into account the inherent flaws in the Microsoft implementation of Alternate Data Streams (ADS) and uses those attributes to create a tool for increased security. The concept is similar to making lemonade from lemons. We're taking an insecure component of the NTFS file system and creating a tool that will provide increased security. Russ and Grifter will be explaining and demonstrating the use of Alternate Data Streams and then discussing an Open Source project which they have currently begun development on.

Grifter has been involved in the scene for over a decade and currently runs 2600SLC, the Salt Lake City 2600 meeting, and DC801 the Utah Defcon meeting; where he often lectures on a range of security related topics. He has been published in numerous online and print publications and has previously been a speaker at several Defcons. He has also been the subject of interviews for various online, print, and television pieces regarding different areas of the hacker culture over the years. He is a Defcon Goon and primary organizer of the Defcon Scavenger Hunt and Defcon Movie Channel.

Russ Rogers is the CEO and CTO of Security Horizon, a Colorado Springs based information security professional services firm and is a technology veteran with over 12 years of technology and information security experience. He has served in multiple technical and management information security positions that include Manager of Professional Services, Manager Security Support, Senior Security Consultant and Unix Systems Administrator. Mr. Rogers is a United States Air Force Veteran and has supported the National Security Agency and the Defense Information Systems Agency in both a military and contractor role. Russ is also an Arabic Linguist. He is a

certified instructor for the National Security Agency's INFOSEC Assessment Methodology (IAM).

Tierra, while still somewhat new to the scene, has been manipulating bits since the 7th grade, and is currently working on his Computer Science degree at the University of Utah. He has been attending 2600 meetings for more than 3 years now in Salt Lake City, and has been helping run the Defcon Scavenger Hunt since Defcon 10 (you'll find him at the Scavenger Hunt table again this year). While working with the DC801 crew on projects such as this, he spends his time mastering his PHP and SQL skills on various personal projects such as TIMAP found on SourceForge.

RF-ID and Smart-Labes: Myth, Technology and Attacks

Lukas Grunwald, CTO, DN-Systems Enterprise Internet Solutions

This talk provides an overview of the RF-ID Smart-Labes, small labels on products with an embedded microchip and an antenna. Smart-Labes store product and serial-number, expiration date etc. and can be read from a distance.

The Industry is planning to put these labels with an international product code on every product within the next decade, effectively replacing the old bar-code system. Some stores already use Smart-Labes, for example certain pharmacies in the US, and in Europe the Metro Group in their Future Store.

At the end of this talk there is a practical demonstration of RF-DUMP, my tool to read and write Smart-Labes, check their meta-data and manipulate it.

Mr. Lukas Grunwald is CTO of DN-Systems Enterprise Internet Solutions GmbH (Hildesheim/Germany), a globally acting consulting office working mainly in the field of security and internet/eCommerce solutions for enterprises. Mr. Grunwald has been working in the field of IT security for nearly 15 years now. He is specializing in security of wireless and wired data and communication networks, Forensic Analysis, Audits and Active Networking. Mr. Grunwald regularly publishes articles, talks and press releases for specialist publications. He also participates actively in conferences such as Hackers at Large, Hacking in Progress, Network World, Internet World, Linux World (USA/Europe), Linux Day Luxembourg, Linux Tag, CeBIT Conference.

Down with the RIAA: Musicians Against the Recording Industry

Nathan Hamiel (Ichabod Ver7)

Down with the RIAA is a look at the current state of the music business and where it is headed. The presentation uses statistics and facts to map out where the industry currently is and details the problems with the current model. After the problems with the current model are shown then the groundwork for the future of the music business is laid out showing how the recording industry is no longer needed. Included in the presentation is information on how artists can produce their own music cutting out the recording business.

The recent increase in quality and decrease in price of recording equipment has made it very feasible for artists to make very high quality recordings on their own. This is the way of the future, and the processes are detailed by an independent music producer with experience in the field. Most people do not know it is possible to make quality recordings that rival commercial ones from your apartment, without even disturbing your neighbors. People are screaming for a change in the music industry. With all of the problems that the RIAA is creating for the music consumer, consumers will begin to be open to a new model where the hassles of the RIAA will no longer be an issue. The future of the music business will also afford more opportunity to artists leveling the playing field and decreasing competition between artists.

Nathan Hamiel (Ichabod Ver7) is an independent artist and producer living in Jacksonville, FL. As an artist he has shared the stage with acts such as The Union Underground, Fuel, Scrape, 8Stops7, Phoenix TX, The Crux Shadows, and many more. Using his skills gained as a recording engineer hehas been able to create high quality recordings using very reasonably priced equipment many times surpassing the quality of commercial recordings. He has many albums and recordings to his credit and shares the knowledge with other artists and producers world wide. He has created some of his own techniques, including ones on layering drum samples that can now be heard on many different recordings. On the technology side, he is a CISSP, was a presenter at Interz0ne 3, and VP of the Jacksonville 2600.

Subliminal Channels In Digital Signatures -or- Why it's VERY Important To Verify Trustworthiness of Encryption Programs

Seth Hardy

A number of papers about a subliminal channel in the Digital Signature Algorithm were published more than ten years ago, allowing for communication through digital signatures in an undetectable manner. The subliminal channel is generally viewed as a method of legitimate but hidden communication, but it can also be used for leaking secret information (such as keys) in a undetectable way to anyone who knows what to look for. I will present on how this subliminal channel works, and demonstrate using a patched version of the GNU Privacy Guard how to use it for both benign and malicious reasons, both of which have little to no prior implementation in encryption programs.

Seth Hardy is involved in both research and implementation in the field of cryptology, both as part of a university research group and independently. His primary interest is the mathematics side of crypto, so he's been involved in a number of projects which involve translating new and better concepts from math into a working implementation in code. Seth has presented his work at a number of conferences, usually with his good friend Jose.

The Insecure Workstation

Deral Heiland

The insecure workstation. A creative look at the windows group policies as a security solution in today's workplace and how easily they are circumvented. This talk will discuss the Were, What and Why on policies and also demonstrate simple tricks to bypass policies and exploiting poor policy implementation.

Deral Heiland has been in the IT field since 1994 working in the following industries; Newspaper media, System Integrator, Manufacturing. Held the following position Network Administrator, Financial systems manager, Network field engineer and Network Security Analyst. He presently holds the following certifications SSCP, CCNA, CCWS, CNE5 and CWSE.

Smart Card Security: From GSM to Parking Meters

h1kari

Smart Cards are used all over the place in every day life. The unfortunate (or fortunate) side of Smart Cards is that most widely deployed systems don't use any real security and rely mostly on obscurity. This presentation will discuss the different types of Smart Cards, exactly how to reverse engineer the protocols they use, and how to exploit their security weaknesses. For demonstration, we will look at GSM SIM Cards and San Diego Parking Meter Debit Cards and show how their security can be defeated.

h1kari has been in the security field for the past 5 years and currently specializes in 802.11b Wireless Security, Smart Card, and GSM development specifically to exploit its various inherent design weeknesses. He is the main developer of the bsd-airtools project, a complete 802.11b penetration testing and auditing toolset, that implements all of the current methods of detecting access points as well as breaking wep on them and doing basic protocol analysis and injection. David has spoken at numerous international conferences on wireless security, has published multiple whitepapers, and is regularly interviewed by the media on computer security subjects.

h1kari is also the founder of Nightfall Security Solutions, LLC and one of the founding members of Dachb0den Research Labs, a non-profit southern california based security research think-tank. He's also currently the chairman of ToorCon Information Security Conference and has helped start many of the security and unix oriented meetings in San Diego, CA.

Blind SQL Injection Automation Techniques

Cameron "nummish" Hotchkies, 0x90.org

Due to improper software design and implementation practices, the number of web-based applications vulnerable to SQL injection is still alarmingly high. Yet the actual steps used to exploit these applications remain very tedious and repetitive. This presentation will focus on methods available to automate the task of exploiting blind sql

injection holes. It will also feature a new tool, "SQueaL" and explain some of the research, used in the creation of this tool as well as ideas for expansion on the tool or other uses of the core libraries developed.

Cameron Hotchkies, aka nummish, is a member of the 0x90.org digital think-tank and head developer of the new blind injection tool, SQueaL. In his non-free time, he works as a web-application developer and has witnessed (and had to repair) great atrocities in web application design. This has left him a bitter and frail shell of his former self. Some people have suggested he get out more. He is currently struggling to write code to teach him how to properly pronounce the word "about". This will be his first time speaking at DEFCON.

NoSEBrEaK—Defeating Honeynets

Thorsten Holz, Laboratory for Dependable Distributed Systems (RWTH Aachen University)
Dipl.-Jur. Maximillian Dornseif, Laboratory for Dependable Distributed Systems (RWTH Aachen University)
Christian Klein, University of Bonn

Honeynets are one of the more recent toys in the white-hat arsenal. They are usually assumed to be hard to detect and attempts to detect or disable them can be unconditionally monitored. Sometimes it is even suggested that deploying honenets is a way to incerase security. We scrutinize this assumption and demonstrate a method how a host in a honeynet can be completely controlled by an attacker without any substantial logging taking place. We show how to detect honeynets, circumvent logging on a honeynet and finally 0wn a honeynet hard disabling all of a honeypots security features and present the tools to do so.

While being fairly technical the a basic knowledge how shellcode and the like works should be enough to follow the talk.

Thorsten Holz is a research student at the laboratory for dependable distributed systems at RWTH Aachen University where he is trying to bring a solid scientific foundation to Honeynet research.

Maximillian Dornseif and Christian N. Klein have studied computer science at the University of Bonn, Germany; Dornseif also holds a degree in laws. Both are involved in computer security and the German computer underground, namely the Chaos Computer Club, for a long time and are doing security consulting together since the late nineties. Their clients include the industry like Deutsche Telekom and T-Mobile but also government.

Virus, Worms and Trojans: Where Are We Going?

IcE tRe

It seems that the major target of most online bugs is actually quite the same. Over and over again the uninspired, pop the box, seems to be what most writers are after.

In this talk I will explore a bit of virus history in relation to goals, starting with older viral intentions, moving to what appears to be the intentions today and what possibly could be the intentions tomorrow.

This talk will be fairly abstract and I will setup the examples that I use so no previous knowledge will be needed other than a basic idea of how viruses work and what damage they can cause. This information, most people already have from the coverage gleaned from your average newscast, if not other places.

This talk in particular, should appeal to the broadest audience.

IcE tRe, Like many of the people attending DefCon has been involved with networking/internet/'new media' since the early 90's. Working with 2 major unnamed ISP over the years has helped these companies weather the storm of the past 10 years of viruses, ddos attacks and various other security problems.

Black Ops of TCP/IP 2004

Dan Kaminsky, Senior Security Consultant, Avaya Enterprise Security Practice

Continuing the research done in previous years on advanced protocol manipulation and the high speed evaluation of large network characteristics, this year's Black Ops of TCP/IP goes into new territory with a deep analysis of the Domain Name System. A core element of

the TCP/IP application suite, it is everywhere—and there is unexpected power contained within.

Interesting Facets of the Global DNS Architecture: A high speed scanner for DNS servers, modeled after my TCP scanner "scanrand", recently executed several Internet-scale sweeps of the net. Surprising results, with direct implications for computer forensics operations, will be discussed and analyzed.

Distributed, High Speed, Large File Dissemination via DNS, A.K.A. "Reinventing the Square Wheel." Although there have been previous attempts to serve files over the DNS architecture, none have been even remotely usable. I will discuss a new approach that, through its significant performance improvement, is indeed remotely usable.

One-To-Many Streaming Data Dissemination over DNS: The previous system maximizes speed at the expense of making streaming impossible. We will discuss an interesting alternate approach that almost usefully distributes streaming audio data to endpoints via their DNS queries.

SSH over DNS: I will demonstrate a cross-platform, userspace mechanism for moving SSH data over DNS queries. This has implications for captive wireless portals, which often allow bidirectional DNS traffic.

To complete this work, some enormously complex data needed to be understood, and tools were worked with and written towards that end. Experimental 3D information visualization mechanisms and tools are thus available to be demonstrated, extending from using a 3D renderer usually used for MRI medical data as a generic static 3D canvas to using a custom OpenGL particle plotter to dynamically plot multidimensional factors of incoming data streams. A number of other topics will be raised as well, including:

Uses and abuses of remotely visible incrementers and decrementers (such as the IPID field in many TCP/IP stacks, and initial TTL values on arbitrary DNS queries)

Uses of generic packet race conditions, whereby useful information can be gleaned from which packet of a relatively large set effects the state change

Protocol transliteration between TCP and UDP, allowing unreliable communication over what appears to be a TCP session, and allowing reliable data to be transmitted, with zero data expansion, over a UDP link.

Potential solutions to the SSH bastion host security problem, whereby the invocation of remote ssh binaries at a firewall or "bastion host" opens up a single point of major failure for a server infrastructure.

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, and 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", 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.

The Hacker Foundation: An Introduction

Jesee Krembs (aka Agent X), Acting Operation Manager, The Hacker Foundation

Nicholas Farr, Acting Secretary, The Hacker Foundation

The Hacker Foundation (THF) is a non-profit organization dedicated to establishing and maintaining a research and service organization to promote and explore the creative use of technological resources.

Simply put, we want to help people do useful things with technology. This announcement is a formal launch of the foundation. There will be a brief statement about the foundation's goals, operations and how the foundation can work for you.

Jesse Krembs is a Defcon Speaker Goon. He's a cofounder of The Hacker Foundation.

Nicholas Farr: After an academic career focusing on memetic sociology and HCI, most of Nicholas Farr's professional career has been in non-profit management. Administrative work in academia, public radio and computer recycling strengthened his ability to navigate difficult bureaucratic situations. He works on The Hacker Foundations administrativa between MBA classes, press assignments and accounting work for a defense contractor in Michigan.

Bluesnarfing—The Risk From Digital Pickpockets

Adam Laurie, CSO and Director, AL Digital Ltd
Martin Herfurt, Researcher, Salzburg Research Forschungsgesellschaft m.b.H and Lecturer, Salzburg University of Applied Sciences and Technologies

In November 2003, Adam discovered serious flaws in the authentication and data transfer mechanisms on some bluetooth enabled devices, and, in particular, mobile phones including commonly used Nokia, Sony Ericsson and Motorola models. Shortly thereafter, Martin Herfurt of Salzburg Research Forschungsgesellschaft mbH expanded on these problems, and teamed up with Adam to investigate further.

This talk will cover the issues arising out of these flaws, including loss of personal data, identity theft, phone tapping, tracking, fraud and theft of service. The threat to individuals and corporates will be examined, and statistics and examples from the real world presented, as well as live demonstrations of each of the problems. Details of how the industry reacted, what they did, didn't and should have done will also be discussed.

This will be a fun talk and a real eye-opener for those with bluetooth enabled devices.

For further background information on the issue, see:http://www.thebunker.net/release-bluestumbler.htm

Adam Laurie is Chief Security Officer and Director of AL Digital Ltd. and The Bunker. He started in the computer industry in the late Seventies, working as a computer programmer on PDP-8 and other mini computers, and then on various Unix, Dos and CP/M based micro computers as they emerged in the Eighties. He quickly became interested in the underlying network and data protocols, and moved his attention to those areas and away from programming, starting a data conversion company which rapidly grew to become Europe's largest specialist in that field (A.L. downloading Services). During this period, he successfully disproved the industry lie that music CDs could not be read by computers, and, with help from his brother Ben, wrote the world's first CD ripper, 'CDGRAB'. At this point, he and Ben became interested in the newly emerging concept of 'The Internet', and were involved in various early open source projects, the most well known of which is probably their own—'Apache-SSL'—which went on to become the de-facto standard secure web server. Since the late Nineties they have focused their attention on security, and have been the authors of various papers exposing flaws in Internet services and/or software, as well as pioneering the concept of re-using military data centres (housed in underground nuclear bunkers) as secure hosting facilities. Adam has been a senior member of staff at DEFCON since 1997, and also acted as a member of staff during the early years of the Black Hat Briefings.

Martin Herfurt is a researcher at the Salzburg Research Forschungsgesellschaft m.b.H and lecturer in Telecommunications Engineering Degree Program at the Salzburg University of Applied Sciences and Technologies.

He completed his Telecommunications Engineering Degree at the Salzburg University of Applied Sciences and Technologies in 2001. Alongside his study Martin was involved in numerous industry projects, providing him with commercial programming practise.

Since the second half of 2000 Martin has been working as a full time researcher at Salzburg Research Forschungsgesellschaft m.b.H. His project responsibilities range from the co-ordination of a European IST project with a total budget of over 5 million Euro to software agents development.

Together with a Salzburg Research colleague, Martin began in the summer of 2003 a class on mobile data services at the Salzburg University of Applied Sciences and Technologies.

Martin is also currently working on a PhD in computer science at the University of Salzburg.

As part of his fascination with the rapid development in computer programming Martin has become a regular participant in the Chaos Communication Congress which is a yearly meeting of the German hacker association CCC.

Google Hacking][- The Return of the Googledorks

j0hnny long, ihackstuff.com

Google hacking is not new, but it's back and deadlier than ever. This talk is the follow-up to last years very successful talk "Watching the Watchers". Attendees will learn the tricks and tactics that any self-respecting Google hacker should know. Expanded extensively since last year, the techniques and always killer examples from the "googledorks" database are always a crowd-pleaser. Witness how sites from all over the net fall victim to seemingly impossible searches from hackers armed with only the world's hottest search engine. A special "security" section this year covers how to find everything from usernames and passwords to live IDS data, live vulnerability scanner output and SQL injection points. This talk intends to spread the word and help protect the security community from this dangerous and eye-opening form of information leakage.

j0hnny long "sold out" many years ago by accepting an I.T. position within a major international company. By promptly securing each and every site he breaks into, Johnny has managed to maintain his friendships with hackers on both sides of the security fence. Regardless of the color of his hat, Johnny is still passionate about hacking, and it shows through his work, his website and especially through his presentations which consistantly secure rave reviews.

Phreaking in the Age of Voice Over IP

Lucky 225, Default Radio

Strom Carlson

Phreaking in the age of Voice Over IP? What the hell is Voice Over IP? If you're asking this question and you're interested in phones and thought phreaking was dead back in the early '80s when blueboxing died, or 2002 when AT&T killed redboxing on long distance calls then this is the speech for you. Or if you know what VoIP is but want to know how the hell it has any impact on phreaking you should also attend. This talk intends to educate it's audience on the new age phreakers. Most of the discussion will involve a detailed explanation of Calling Party Number(CPN), ANI, and Caller ID, and the differences between all three, we will also be covering the basics of phreaking with Voice Over IP technology, Asterisk, and VXML.

Not all of this presentation will be dealing with VoIP, this is a basic new age phreaking presentation that will show the latest techniques that phreaks are using today—it's not just about free calls either, hell you get that with VoIP anyways! You will learn not only why VoIP is important, but such things as Spoofing Caller ID(and no we don't mean orangeboxing, Social Engineering Telus, our methods are simple to use and will cost as little as $15/month)

As technology is rapidly changing, so is our phone system. We will be discussing a basic over view of Voice Over IP and some of the services provided by many of these so-called "Broadband phone companies." We will also be discussing Calling Cards that use VOIP technology to provide cheaper rates to their customers. We intend to explain how VoIP is changing the phone system and making it very easy for the every day consumer to spoof Caller ID by spoofing Calling Party Number(CPN), and how this can be exploited to circumvent security in such things as Voicemail, Credit Card Activations, and even Telephone company numbers that when you call from your "own phone" will give you complete control over your dial-tone telephone line. We also plan on showing how easy it is to get around services like "Call Intercept" without even spoofing Caller ID. We will also be discussing why *67 and Complete Caller ID block features offered from the phone company are not adequate privacy protection as anyone can still get your phone number when you call them with your number blocked, we'll of course describe how this can be possible. As time

permits there may very well be much more, you wont want to miss this presentation.

Lucky225 is the co-host of an internet streaming radio show 'Default Radio' that streams on Rant Radio a free non-profit shoutcast server that has been running for 6 years). He has been a writer for 2600 magazine since 1999 and has spoken at both H2K2 and Defcon 11. He has been an avid phone phreak since his early teens in High School and has much experience with the telephone system and a wide variety of knowledge ranging from regular telephones, payphones, cell phones, and voicemail systems to ANI, Caller ID, PBX's, switches, VoIP and much more.

Strom Carlson is one of the last true phone phreaks; he has an intense interest in the structure and history of the telephone network and an intense distaste for fraud, theft, and vandalism. 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 learn what they're really talking about; he also encourages you to listen to everything on http://www.phonetrips.com/ and to poke around http://www.stromcarlson.com/

Smile, You're on Candid Camera: The Changing Notions of Surveillance in Postmodern America

Kevin Mahaffey
Flexilis

Recently, surveillance has become somewhat of a pop-culture fascination. From the Reality TV shows permeating every network's line up to the webcam phenomenon of the late 1990s, surveillance has become more a source of entertainment than ever before. Benjamin Franklin's quote, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety," has long served to exemplify the American, "Big Brother," notion of surveillance: that the government is the main aggressor and seeks to take away privacy and thereby, liberty. My talk will contrast traditional perceptions of surveillance in American culture with new notions brought forth in the emerging digital economy. The privacy of individuals is being bought from individuals through tangible or intangible rewards and resold as demographic data to the highest bidder. Instead of resisting the reduction of privacy, people are embracing surveillance as a benign improvement of everyday life. If we continue such a trend, will society be better for it, or will ubiquitous surveillance serve to implement Orwell's nightmare in 1984?

Kevin Mahaffey is an Electrical Engineering student at the University of Southern California. He has conducted extensive research regarding the sociological effects of the growth of commercial surveillance in American culture. When not confusing sociology with technology he is the Director of Software Development for Flexilis and is currently developing a few Bluetooth security tools hopefully to be released this year at Defcon. He also writes the occasional article for DailyWireless.com and has 6 years of experience working in commercial internet technology.

Snake Oil Anonymity: How To Spot It, And How Not To Write It

Nick Mathewson, Lead Developer, Mixminion and Core Developer, Tor Anonymyzing Proxy

Much software that promises "anonymity" fails to deliver, as witnessed by a succession of compromised file-trading networks, back-doored communications systems, overhyped vapornets, and insecure "improvements" on existing remailer networks. I'll discuss a bunch of allegedly anonymous systems, and explain how a clever attacker can defeat each of them. Audience members will learn to recognize the warning signs of broken anonymity in anonymous communications and P2P; and will learn a few principles to help them design the anonymity properties of their own systems.

Nick Mathewson is one of the main designers on Type III (a.k.a. Mixminion), the protocol that will replace the one currently used by the Mixmaster anonymous remail He is also the lead developer of the Mixminion software, and a core developer on the Tor anonymizing proxy.

Hack the Vote: Election 2004

Rebecca Mercuri, Ph.D.
Bev Harris, author of "Black Box Voting: Ballot-Tampering in the 21st Century"

In the rush to solve problems that emerged from Florida's Presidential election dispute in 2000, computerized voting systems have been deployed in unprecedented numbers. Estimates indicate that 30% of the USA will be voting on fully electronic equipment offering no capability for independent recounts, and another 50% of the country will be casting ballots tabulated by computer-based scanners. Vendors and promoters of these systems have made promises of reliability, accuracy and accessibility. Yet evidence from the 2004 primary season and earlier uses in 2002 and 2003 elections have demonstrated malfunctions resulting in irretrievable loss of vote data, usability issues including county-wide denial of service incidents, and fraud allegations due to software substitutions. This talk will explore the vulnerabilities of electronic voting systems to insider and outsider attacks, along with the possibilities and ramifications of large-scale vote fraud in the 2004 election and beyond.

Dr. Rebecca Mercuri became an overnight celebrity during the media frenzy that ensued when the U.S. Presidential election ended in a dead heat in November 2000. A few weeks earlier, she had successfully defended her Doctoral Dissertation "Electronic Vote Tabulation: Checks and Balances" at the University of Pennsylvania, and then found herself writing testimony in the now-legendary Bush v. Gore case that was working its way through the legal system. Her testimony was presented to the U.S. 11th Circuit Court of Appeals and referenced in the briefs to the U.S. Supreme Court. Since then, she has provided formal testimony on voting systems to the House Science Committee, Federal Election Commission, U.S. Commission of Civil Rights, and the U.K. Cabinet, has been quoted in the U.S. Congressional Record, and has played a direct role in municipal, state, federal, and international legislative initiatives. Rebecca's comments on election technology are frequently cited by the media, and she authors the quarterly "Security Watch" column in the Communications of the Association for Computing Machinery (archived at www.notablesoftware.com). Having recently completed a research fellowship at the John F. Kennedy School of Government in their Belfer Center for Science and International Affairs, Dr. Mercuri will be moving to Harvard University's Radcliffe Institute in the Fall.

artwork by Londo

Bev Harris, author of "Black Box Voting: Ballot-Tampering in the 21st Century," began writing on the subject of electronic voting machines in October 2002. Her investigative journalism has since been cited in The New York Times (three times), and on CBS, Fox News, and CNN. In writing Black Box Voting, Harris spent over two thousand hours researching voting machines, and interviewed hundreds of witnesses including many election officials and even voting machine programmers who work directly for the firms that build these machines. During the course of writing Black Box Voting, Harris discovered that one of the largest voting machine companies, Diebold Election Systems, had committed a massive security breach, leaving thousands of sensitive voting system program files on an unprotected Web site. These files have now triggered a national investigation and activism movement to restore clean, trustworthy voting systems.

DIGEX—At the Dawn of the Commercial Internet

Doug Mohney, Editor, VON Magazine and contributor to Mobile Radio Technology Magazine

Hearken back to the days of yesterday, circa 1993, when men were men, the Internet "backbone" was T3 and run by ANS, and a few brave start-up companies around Washington D.C. were fighting the phone company and each other to build the "commercial" Internet. One of them, DIGEX, literally started out in the founder's basement in '92 and rapidly grew to be a major force in what ultimately became known as web hosting. DIGEX "invented" web hosting, was first to light-up mtv.com, collected a whole bunch of dot.gov sites including one for a Langley, VA-based agency, and grew into a 600+ person company with a 1996 IPO. Doug Mohney was employee #10 at DIGEX and witnessed a whole bunch of stuff from late '93 through 1997.

Doug Mohney was employee #10 at DIGEX. He is often confused with employee #1 (Doug Humphrey; Mohney does not have Humphrey's beard, wife, or bank balance). Currently, he is online editor for VON Magazine and a contributor to Mobile Radio Technology magazine. His first BOARDWATCH article, a history of DIGEX, was published in 1997 to critical acclaim by most and heartburn by a few.

Shoot the Messenger—Using Window Messages to Exploit Local win32 Applications

Brett Moore, CTO, security-assessment.com

The windows GDI interface uses messages to pass input and events to windows. As there is currently no way of determining who the sender of the message is, it is possible for a low privileged application to send messages to and interact with a process of higher privilege.

This presentation will cover in details some of the flaws exposed through these messages, and demonstrate how they can be exploited to conduct privilege escalation and other attacks. Attendees should be familiar with the shatter attack concept and may want to review the following documents before attending:

Shatter Attacks—How to break Windows, Chris Paget
Win32 Message Vulnerabilities Redux, Oliver Lavery
Shattering by Example, Brett Moore

Brett Moore leads the security research and network intrusion teams at security-assessment.com. He has been credited with the discovery of multiple security vulnerabilities in both private and public software vendors' products including Microsoft web products.

Cracking Net2Phone

Todd Moore, NetWitness Product Manager, Forensics Explorers, ManTech International Corp.

Do you think using Internet Telephony is more secure than a regular phone? Think again! Internet Telephony is becoming more common and those that think it is safer from wiretaps than regular phone communications are wrong. This presentation will demonstrate how to decrypt Net2Phone's dialed phone numbers, and playback fully reconstructed audio conversations from network packet captures. Included will be a demonstration of NetWitness 5.0's VOIP playback capability.

Todd Moore is the product manager of NetWitness®, a commercially available cyber-forensics tool. Moore's extensive knowledge of Internet technologies, network security, and software development helped make NetWitness® well-known for providing powerful insight into network traffic.

Moore has over ten years of professional experience in the field of network security and has extensive experience developing commercial software applications. He has a bachelor in Computer Science from Old Dominion University and is a Microsoft Certified Solution Developer (MCSD). Moore started with CTX Corporation in 1996 securing global intranets and designing network security software to help audit and analyze network traffic. He joined Forensics Explorers, a Division of ManTech IS&T, as Director of Software Development in 1999 and later became the NetWitness® Product Manager.

Moore teaches classes on designing quality software and has made numerous television appearances presenting the latest in technology trends. He has two patent pending inventions in the field of cyber-forensics.

The History of the Future

Robert Morris, former Chief Scientist for the NSA

Mr. 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.

artwork by d master

Counter Intelligence/Counter Espionage - How To Engage and Avoid In The Corporate Network (An Operatives View)

Mudge

The Advantages of Being an Amateur

Brett Neilson

For close to 100 years amateurs have been working with radios and sending transmission all over the world. The dawn of the information age has inspired many new technologies and advancements in communication; and amateur radio is no exception. Today's modern amateur radio operators are building wireless networks and enjoying several advantages over their unlicensed counterparts. This presentation will review some of these advantages as well as talk about some of the newer areas of interest including HSMM and APRS.

Brett L. Neilson is a network security and systems engineer with a strong background in the wireless industry. Currently he is working for one of the world leaders in Intrusion Prevention supporting clients with network security related issues. He previously worked for one of the leading wireless communication companies as a Senior Systems Administrator and RF Field Technician. While there he worked to develop, deploy, and maintain their national infrastructure. Some of his work is currently published in two information security related books, Maximum Wireless Security & Maximum Security 4th Edition. Mr. Neilson is a former member of the North Texas FBI Emergency Response Team (InfraGard) and is an FCC-licensed amateur radio operator. In these roles he has worked with multiple government agencies providing emergency communication assistance and coordination.

Better than Life—Manipulation of The Human Brain With The Use of Machines

Ne0nRa1n
John McClintock

Just as the understanding of the human genome will soon allow us to control the essential physical processes that create our bodies, knowledge in the manipulation of the human brain with the use of machines will give us the ability to reconstruct ourselves mentally in a way that has only been imagined by the most outlandish of science fiction writers.

This speech will take you through the history of altered states, from ritual and religion, to drugs and chemicals right through to the future of the technology. You will be introduced to some of the mechanical tools that have existed for years that have only be talked about and affordable by a few. As well as showing you how to build your own home-brew mind machine, the presentation also will also be discussing other brain manipulating technologies.

Ne0nRa1n has been involved in the computer underground for a decade and is also a world traveler and slacker extraordinaire. In her pursuit to understand how brain waves work, she has spent extensive time in a Buddhist hermitage where she was able to experience meditation first hand. Among her current projects is her quest to find a way to replace expensive chemical antidepressants with affordable digital drugs.

Several years back, Jon McClintock received a Computer Science degree from a university of no consequence. Since then, he's bounced back and forth several times between enterprise and embedded software development. Equally comfortable debugging 8-bit microcontrollers using a logic analyser as he is developing highly available, multi-tier applications, Jon enjoys manipulating minds both large and small.

Ask EFF: Discussion and Q/A on the State of Digital Liberties

Annalee Newitz, Policy Analyst, Electronic Frontier Foundation
Wendy Seltzer, EFF Staff Attorney specializing in IP
Kevin Bankston, Equal Justice Rights Fellow at EFF specializing in privacy/surveillance
Seth Schoen, Staff Technologist, Electronic Frontier Foundation
Jennifer Stisa Granick, Executive Director of the Center for Internet & Society (CIS)

The Electronic Frontier Foundation (EFF) is one of the premiere digital liberties organizations in the world. We fight for freedom of expression on the Internet, the right for researchers and consumers to reverse-engineer their devices, expansion of the public domain, and

electronic privacy and anonymity. On this panel, three representatives of EFF will discuss the latest developments in digital liberties, including free speech on the Internet, copyright infringement lawsuits, and electronic surveillance laws under the USA-PATRIOT Act. Audience participation and discussion are part of the deal. Come with your legal and policy questions this is your chance to ask EFF!

Annalee Newitz (www.techsploitation.com) is EFF's Policy Analyst. She talks to the media, conducts research, and writes policy recommendations and white papers. Although she is a digital rights generalist, her special areas of interest are expanding the public domain, free speech, and network regulation. Previously, she was Culture Editor at the San Francisco Bay Guardian, and was the recipient of a Knight Science Journalism Fellowship in 2002. She writes a syndicated column called Techsploitation and is published regularly in Wired, Security Focus and Salon. In her off-hours, she edits an indie magazine called Other (www.othermag.org). She has a Ph.D. in English and American Studies from UC Berkeley.

Wendy Seltzer is a Staff Attorney with the Electronic Frontier Foundation, 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. Wendy speaks frequently on copyright, trademark, open source, and the public interest online. She has an A.B. from Harvard College and J.D. from Harvard Law School, and occasionally takes a break from legal code to program in Perl.

Kevin Bankston, an attorney specializing in free speech and privacy law, is the Electronic Frontier Foundation's Equal Justice Works/Bruce J. Ennis Fellow for 2003-05. 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.). Kevin received his J.D. in 2001 from the University of Southern California Law Center. Kevin's fellowship at the EFF is sponsored by Equal Justice Works Fellowships and the Bruce J. Ennis Foundation.

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. Prior to Linuxcare, Schoen worked at AtreNet, the National Energy Research Scientific Computing Center at Lawrence Berkeley National Laboratory, and Toronto Dominion Bank. Schoen attended the University of California at Berkeley with a Chancellor's Scholarship.

Jennifer Stisa Granick is 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. Previously, she founded 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 law and technology litigation clinics. Granick continues to consult on computer crime cases and serves on the Board of Directors of the Honeynet Project. She was selected by Information Security magazine in 2003 as one of 20 "Women of Vision" in the computer security field.

Real World Privacy, How to Leave Less of A Trail in Life

n0namehere

Like leaving breadcrumbs in the forest, individuals leave a data trail throughout their day. This talk will look at practical ways to leave a smaller data wake. Privacy isn't dead. Time, money and effort are needed to maintain and live outside the data collection mechanisms that are nowpart of society.

Level of privacy achieved

How easy it is to lose one's privacy...

This is not a talk to look at the ways in which your data is shared, but a look at examples and methods by which one can minimize sharing the data in the first place. Topics to be covered include communications, money, medical, travel, shopping, rubbish and major life events. The key is to not leave any data, but, when one must leave data, leave it in a way which it won't trace back to you.

n0namehere started down the privacy route in the early 1990s after mistakenly hearing cell and cordless phone calls on his recently purchased scanner. Realizing the ease in which others could listen in on his life, this event led to a re-evaluation of his behavior which changed his life. He spreads the word among friends and family, encouraging many down the road to strongerprivacy.

n0namehere is a big computer company survivor whose personal and professional work focuses on computer security and privacy issues ranging from running to designing to breaking systems, networks and applications. n0namehere has worked for Fortune 500 companies, consulted on hundreds of system and network designs and worked security/privacy issues during the Summer Olympic Games. n0namehere doesn't live in a cave but balances privacy and reality in his daily life.

Automotive Networks

Nothingface, Area 49

This presentation provides an introduction to the electronic networks present on late model automobiles. These networks will be described loosely following the OSI model of networking. Common uses of these networks will be presented, and the privacy implications of some uses will be questioned. The presentation will conclude with an introduction to OpenOtto, a free software and hardware project implementing the network protocols previously described.

Nothingface is formally educated in electrical and computer engineering and informally (i.e., not) educated in automotive maintenance and repair. He has been known to earn his keep doing software design, hardware design, and security consulting. Nothingface is currently employed designing hardware and software for two-way radio communication networks.

Mutating the Mutators

Sean O'Toole

Since the introduction of metamorphic stealth in the computer virus world, it has been suggested that the method can also be used to protect any, even legitimate, code. The only downfall of this technique is that how the engine manipulates the code remains constant. This allows the original code to be obtained by using an optimizer. The next step for this stealth method is to create an engine that will change how the code in manipulated. This speech will outline how to create an engine that integrates random code with alternate encoding of an instruction to create a semi-random set of instructions, which will fit into the metamorphic engine paradigm.

Sean O'Toole is fresh out of college for Computer Science and Mathematics. He has been playing around with viruses since high school and had also taken independent studies on computer viruses in college. As well as the above, he also helped institutions such as NCAR use Artificial Life Algorithms for modeling.

Digital Active Self Defense

Laurent Oudot, Computer Security Engineer, Rstack

In a cyberworld of never ending struggles, defenders might have a new weapon in the future in order to defeat attackers. This talk will focus on those possibilities called: digital active (self) defense.

For example, after a compromission, a victim might want to react and even hack back the aggressor. This potentialy natural idea might not be legal most of the time, and many drawbacks exist. Think about the case where an aggressor would use a connectionless attack ; the source of the intrusion could not be the real one (spoofing) so that a retaliation would not be a good idea!

This presentation aims at sharing ideas about digital active self defense to focus on the essential current questions: Why and when should we try to react like that? How could we play with incoming aggressors in order to limit the risks? What would be the limitations of such solutions (legal and technical issues)?

As a conclusion, we will evaluate the potential hidden by those technologies used for Information Assurance and imagine future kind of solutions, digital active self defense systems.

Laurent Oudot (http://rstack.org/oudot/) is a french security expert currently employed by the CEA (Commissariat Energie Atomique) which is the equivalent of the US Dept Of Energy. On his spare time, he is also a member of a security group called "Team Rstack" composed of security addicts and geeks. Laurent's research focus on defensive technologies highly closed to blackhats activities like honeypots, intrusion prevention, intrusion detection, firewalls, sandboxes, mandatory access control, etc.

Laurent is the co-author of several research papers recently published and released on Securityfocus, Institute of Internal Auditors UK, MISC magazine and Linux Magazine France. He has presented at national and international conferences and meetings such as Cansecwest (Vancouver, 2004), Eurosec (Paris, 2004), BlackHat Asia Briefings (Singapore, 2003), Honeynet Project Meeting (Chicago, 2003), Libre Software Meeting (Metz, 2003), FOSDEM (Bruxelles, 2003), etc.

He co-organized security events such as the Libre Software Meeting (co-chairman of the Security Topic with Bradley Spengler from Grsecurity, 2002), Symposium Securite des Technologies de l'Information et de la Communication (SSTIC 2003 and 2004), a Computer Security Summer School (2004), etc.

Laurent has taught network and system security in high schools for engineers and has managed numerous security projects on the last 7 years.

Recently with Nicolas Fischbach, he co-created the French Honeynet Project which is part of the international Alliance of honeynets. Now, Laurent is a member of the Steering Committee of the Honeynet Project leaded by Lance Spitzner.

The DEFCON Surveys

Dr. Larry Ponemon, Chairman, Ponemon Institute.

Ponemon Institute recently conducted two independent surveys concerning individual privacy rights. The first study examines the public's perception concerning the safety and security of e-voting systems. The second study explores the public's reaction to the U.S. government's CAPPS II proposal that requires airlines to share personal data about passengers with the Department of Homeland Security. Dr. Larry will present an analysis that compares and contrasts the "DEFCON" community to members of the general public in terms of perceptions and beliefs about privacy issues.

Dr. Larry Ponemon is Chairman of Ponemon Institute, a "think tank" dedicated to privacy, data protection and information security policy research. He is also serves as an adjunct professor of privacy and ethics at Carnegie Mellon University's CIO Institute and CyLab.

Advanced Netfilter; Content Replacement (ala Snort_inline), and Port Knocking Based on Passive OS Fingerprinting

Michael Rash

The boundaries between network access control devices and network monitoring devices are steadily becomming blured. Network intrusion detection systems are moving into the realm of not only monitoring network traffic, but also modifying it either through dynamic reconfiguration of firewall rulesets, spoofed session-busting traffic, or outright alteration of application layer data (ala Snort_inline). Firewalls themselves are also getting smarter about protocol validation and application layer data. This talk will discuss two main topics; 1) a patch to the iptables string match extension in the Linux kernel that allows iptables to perform the same data substitution as Snort_inline but three times faster, and 2) a new tool called "fwknop" that implements port knocking authentication based on passive operating system fingerprints as detected via iptables log messages. The latter makes it possible to allow only, say, Linux systems to connect to your SSH daemon.

Michael Rash holds a Master's Degree in applied mathematics with a concentration in computer security from the University of Maryland. Mr. Rash works as a security research engineer for Enterasys, Inc. where he develops signatures and writes code for the Dragon IDS. Previous to Enterasys, Michael developed a custom host-based intrusion detection system for USinternetworking, Inc. which was deployed on over one thousand systems from Linux to Cisco IOS. Michael frequently contributes to open source projects such as Netfilter and Bastille-Linux, and has written security related articles for the Linux Journal, Sys Admin Magazine, and Information Security

Magazine. He is also a co-author of the book Snort-2.1 Intrusion Detection published by Syngress (to be published in late May, 2004). Michael is the developer of two open source tools "psad" and "fwsnort" that are designed to tear down the boundaries between iptables and the Snort IDS. More information about Michael and his open source projects can be found at: http://www.cipherdyne.org/

Mixmaster vs. Reliable: A Comparison of Two Anonymous Remailer Applications

Len Sassaman

The "Type II" remailer network has been operating since 1995, providing strong anonymity email services to the public. We recently performed an analysis of the anonymity provided by the two independent implementations of the Type II protocol. This is joint work with Claudia Diaz and Evelyne Dewitte, to be presented at the ESORICS conference in September.

This talk will discuss the methods used to evaluate the anonymity provided by Mixmaster 3.0 and Reliable 1.0.5. It will explain the threat models considered for email anonymity and known attacks agaist them, highlight the differences in the mixing algorithms used, identify potential areas of weakness in the applications, and explain the reasoning behind the different design decisions in the two applications.

Len Sassaman is a communication security consultant specializing in Internet privacy and anonymity technologies. Formerly the security architect for Anonymizer and a software engineer for PGP Security, Len is now focusing on research in the area of practical attack-resistant anonymity systems which can be widely deployed and used by large groups. Additionally, Len is an anonymous remailer operator, and maintainer of the oldest actively-used anonymity software, Mixmaster.

artwork by flavah

Digitizations And Documentary

Jason Scott, Webmaster, TEXTFILES.COM,Director, BBS Documentary

Jason Scott of TEXTFILES.COM, a site dedicated to the history of Dial-Up Bulletin Board Systems, embarked on a quest to film an all-inclusive BBS documentary in 2001. What started out as a one-year project grew to three, and what started as a two-hour film will be a six-hour series. Thousands of miles of travel and 200 interviews later, the production is now nearing the end of editing and the release date. Jason tells you what he learned, why you shouldn't hesitate to make your own projects, and the occasional story that technically can't be mentioned in the film.

Jason Scott is the creator and webmaster of TEXTFILES.COM, a website dedicated to collecting the files and related materials from the era of the Dial-up BBS. This website, originally built from files he collected as a BBS user in his early teens, has expanded to many gigabytes of data and now recieves thousands of visitors a day.

Inspired to create "the ultimate BBS list" from the hundreds on his website, he suddenly started recieving dozens of stories from BBS users and operators who found their old BBSes listed among others. Recogizing a missing piece in the story of computers, Jason used his dormant filmmaking skills (Emerson College Film Degree, 1992) to create this documentary.

When the Tables Turn

Sensepost

Until now network security defences have largely been about building walls and fences around the network. This talk revolves around spiking those walls & electrifying those fences! During this talk we will highlight techniques (and tools) that can be used to turn the tables on prospective attackers with passive-Strike-Back. We will explore the possibilities across the assesment spectrum responding to the standard assesment phases of Intelligence gathering, Reconnaissance & Attack with Disinformation, Misdirection, Camouflage, Obfuscation & Proportional Response.

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. He studied Computer Science at UNISA, Mathematics at the University of Heidelberg in Germany and has a Diploma in Information Security from the Rand Afrikaans University. He is an accredited BS7799 Lead Auditor with the British Institute of Standards in London. 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.

Hacking the Spectrum: Open Source Software vs. the Broadcast Flag

Wendy Seltzer, Staff Attorney, Electronic Frontier Foundation
Seth Schoen, Staff Technologist, Electronic Frontier Foundation

The FCC, at Hollywood's request, has mandated a broadcast flag for high-definition digital television (HDTV). By July 2005, it will be unlawful to sell devices that don't respond to a "do not copy" flag or that provide unencumbered high-definition digital outputs. The flag's "robustness" requirement will make it impossible to build an open-source HDTV version of the TiVo. This talk will demonstrate how these rules thwart user innovation, showing an open-source HDTV PVR (MythTV on Linux) you soon won't be able to build. We'll discuss the law and challenges to receiver regulation, and encourage people to get HDTV cards while they still can.

Wendy Seltzer is a Staff Attorney with the Electronic Frontier Foundation, 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. Wendy speaks frequently on copyright, trademark, open source, and the public interest online. She has an A.B. from Harvard College and J.D. from Harvard Law School, and occasionally takes a break from legal code to program (Perl).

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. Prior to Linuxcare, Schoen worked at AtreNet, the National Energy Research Scientific Computing Center at Lawrence Berkeley National Laboratory, and Toronto Dominion Bank. Schoen attended the University of California at Berkeley with a Chancellor's Scholarship.

Wireless Weaponry

The Shmoo Group, featuring: Bruce Potter, Beetle, Cazz, Bob Fleck, Eric Johanson, Mike Messick, Myles, Holt Sorenson, and Rodney Thayer

From the same crazy folks who brought you Airsnort, Airsnarf, Bluesniff, Fine Tooth Comb, HotspotDK, and yes, the HackerBot, comes the annual deluge of wireless wackiness. The Shmoo Group takes a break from beer, Root-Fu, and their constant media-whore campaign to just give Shmoo shtuff away, and it's all wireless-related for you RF rogues. Updated hardware. Updated software. Blah, blah, same old

boring sh—WAIT! What's this?! NEW hardware? NEW software? OMFG. Bow before the Sniper Yagi! Bork all sorts of "secure" wireless networks with new tools from the Shmoon! It's time to update your kick-ass arsenal, folks! If you're a "Wireless Warrior", TSG has your "Wireless Weaponry"—and a saved-for-DefCon announcement sure to make the Shmoo in you rejoice!

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 Root-Fu, 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.

A Comparison of Buffer Overflow Prevention Implementations and Weaknesses

Peter Silberman, Security Engineer, iDEFENSE
Richard Johnson, Senior Security Engineer, iDEFENSE

Buffer overflows are historically the most commonly exploited software vulnerability in the security world. The last year has seen effective automated attacks such as the MS Blaster worm and SQL Slammer worms. Due to the rapid growth of worm technology and readily available automated worm generation tools, the need for buffer overflow protection software has dramatically increased.

This presentation will give the attendee an overview of the methods used by current stack protection technology.

We will discuss the varying types of stack overflow protection available for the Linux and Windows operating environments and the weaknesses that lie within each implementation. This will also be the first public discussion of available third-party buffer overflow prevention software for the Windows operating system. The test suite used to analyze the exploitability of common software vulnerabilities has been modified with specialized shellcode to be used against buffer overflow protection methods. A demonstration will be provided and the tool is available to attendees.

The attendee should have basic knowledge of buffer overflow exploitation, but the presentation will build on itself, and in the end offer a tool that anyone can use to test their buffer overflow protection software.

Peter Silberman is a Security Engineer at iDEFENSE. Peter works in the iDEFENSE labs where he conducts vulnerability research in between going to high school. He is especially interested in advanced exploitation of the win32 platform, buffer overflow protection methods, and windows forensic analysis. Peter has been a professional vulnerability researcher for a year, and has spent two or three years as an independent researcher.

Richard Johnson is a Sr Security Engineer at iDEFENSE. He works in the iDEFENSE Labs where he is responsible for conducting vulnerability research, malicious code analysis, and developing reverse code engineering tools and methodologies. Areas of interest include run-time process modification, live kernel patching, embedded systems reverse engineering, and seeing how much beer a man can drink in an evening.

Bubonic Buffer Overflow

spoonm, Digital Disaster Inc.
HD Moore, Hack Master Supreme

The Metasploit Framework has progressed from a simple network game to a powerful tool for administrators and security analysts alike. Over the past several months, the Framework has been enhanced with improved exploit techniques and a truly advanced suite of payloads. This presentation provides a background on what exploit frameworks are, what they can provide you, and why you should be using one. A live demonstration will highlight many of the advanced features of the Framework, describe how they can be used to accomplish a variety of tasks, and show that the technology for "hacking like in the movies" is already available today. Attendees will be provided with an early-access copy of version 2.2 of the Metasploit Framework; which includes a number of techniques and exploit modules that are not

publicly available anywhere else. Additionally, this release is the first version of the Framework to include a development kit for creating your own custom modules.

Spoonm is currently pursuing a Bachelors degree in Software Engineering. Much to the detriment of his early morning classes, he is an active researcher in many different security areas, most notably in the exploitation and post-explotation process. He has developed several post-exploitation tools, and between working as a security consultant, and asm wielding, he currently spends most of histime working on the Metasploit Framework.

HD Moore is one of the founding members of Digital Defense, a security firm that was created in 1999 to provide network risk assessment services. In the last four years, Digital Defense has become one of the leading security service providers for the financial industry, with over 200 clients across 43 states. Service offerings range from automated vulnerability assessments to customized security consulting and penetration testing. HD developed and maintains the assessment engine, performs application code reviews, develops exploits, and conducts vulnerability research.

CryptoMail Encrypted E-Mail for All (Including Grandma)

Joshua Teitelbaum, Lead Developer, CryptoMail.org
Peter Leung, Webmaster & Project Manager, CryptoMail.org

Four years ago, CryptoMail introduced the first secure open source web based email solution. System administrators and hostile parties no longer had the ability to read a users email. With functionality similar to Hushmail, the world was introduced to an open source solution that they themselves could host.

At Defcon 12, CryptoMail.org will be releasing to the public a major advance in its technology. Users will now be able to transparently and securely communicate with PGP users. Users will be able import their private PGP key set upon account creation as well as external PGP public keys.

Architect Joshua Teitelbaum and project manager Peter Leung will present the overall design of the architecture, the infrastructure and the logistics of the upcoming CryptoMail Email System release. We will demonstrate the technology integration inside the new release for the first time. At the conference, you will have the chance to preview the new release.

Joshua Teitelbaum developed the CryptoMail Email System and founded CryptoMail.org in 2000. Joshua is the primary developer and technical lead of the Email system. He communicates with other developers and members around the world to discuss future features and improvements to the CryptoMail Email System. Besides information security, Joshua holds an active interest in building scalable trading systems for broker/dealers and portfolio managers.

Peter Leung joined CryptoMail.org in 2000 as the webmaster and the project manager.His main task in the organization is to direct, manage, and organize the software release process. Peter collaborates with other members to document the Email system and informs everyone about the organization's activities. Peter holds a BS in mechanical engineering, BS in mathematics, and MBA from SFSU

Quantum Hacking: In Search of a Unified Theory

Richard Thieme,Thiemeworks

The search for a unified theory of everything in contemporary physics stems in part from the fundamental inability to reconcile quantum physics and relativity theory. This has pushed research toward complex mathematical models such as string theory in an effort to model a single way of looking at everything.

The same can be said of the distribution of power in networks and hierarchies. The individual person looks like one kind of thing when viewed in the context of a network and another kind of thing when viewed in the context of a hierarchy. This is analogous to describing a photon as both a particle and a wave. The context of our inquiry determines the content that results and the primary object of that inquiry, the "individual person," is revealed to be a social construction, not an empirical fact.

The lack of a unified theory of humanity and computing is one reason we experience cognitive dissonance today. The notion of the "individual person" is central to current debates about privacy,

intellectual property, and the legality or illegality of network aggression ("black hat hacking"), but from the point of view of the distributed network, there is no individual person, there are only nodes in the network.

In addition, we all inhabit nodes in multiple networks simultaneously. We can field any network-determined identity we choose but we do not determine an individual identity until we choose a network identity. That choice is made in the moment in which we act, so paradoxically, while context determines content, choice is always prior to context and creates it. Until we choose, it is impossible to predict with certainty which choice will be made and therefore what identity will be fielded. This is why security based on perimeter defense or authentication is by definition a failed model.

This analysis has profound implications for traditional notions of free will, loyalty, citizenship, and security. It explains why hackers who evolve from working in online meritocracies to working in corporate structures literally become different people. It explains why a disciplined hierarchical structure like the military can use network centric warriors and fight networks with networks while maintaining a basic identity—for the moment—as the machinery of a nation state. It explains why perspective is worth fifty points of IQ and why perception management creates perspective. It provides one more example in support of Alfred North Whitehead's assertion that "the major advances in civilizations are processes that all but wreck the societies in which they occur."

We are in search of a unified theory of an emergent multi-nodal cyborg personality and how it exercises power. This theory must address hierarchical and distributed structures and what they mean for human identity, law, and global organization and geopolitical strategy. What are the genuine sources of our power? What is the point of reference from which that power is exercised? Who do we believe ourselves to be in the moment in which we act and how do we thereby define ourselves not in theory but in practice, not in the chat room but on the field of action? And finally, why is knowing that we are doomed to fail the key to victory?

Richard Thieme shows how boundaries have morphed, power has been redefined, and The Matrix is more than a movie. Not since Blade Runner has a film described so well the territory that must be crossed. Owning our own souls is the ultimate intention of Third Generation Hacking, the only end that justifies the means.

Thieme holds nothing back as he addresses the deeper implications of what it means to be the network. The stakes are high and the battle is worthy of our best efforts. This talk is a call to arms to accept responsibility for the life and death battle being waged for the hearts and minds of digital humanity.

Exploring Terminal Services, The Last 12 Month of Research. Or, The Evil Admin And His Tools

Ian Vitek, Journalist, Patrik Karlsson

Got shell? On a Citrix or Terminal Services server? The speech will demonstrate some common ways to explore Terminal Services. Uploading files with the keyboard and elevate luser rights to SYSTEM.

How secure is it for a client to connect to a Citrix or a Terminal Services server if an evil admin owns the box? Tools and exploits will be released.

Ian Vitek:183 cm.80 Kg.Brown eyes. Brown hair. Eats meat. Drinks almost every beer you buy him. Interested in layer 2 network security (writer of macof).

If you approach Ian he probably wants to talk about privilege escalation or web application security.

Frustrating OS Fingerprinting with Morph

Kathy Wang, Syn Ack Labs

Sun Tzu once stated, "Know your enemy and know yourself, and in a hundred battles you will never be defeated." By denying outsiders information about our systems and software, we make it more difficult to mount successful attacks.

There are a wealth of options for OS-fingerprinting today, evolving from basic TCP-flag mangling tools such as Queso, through the ICMP quirk-detection of the original Xprobe, and the packet timing analysis of RING, to today's suite of multiple techniques employed by nmap. The ultimate advantage in the OS-detection game lies with the defender, however, as it is they who control what packets are sent in response.

Morph is a BSD-licensed remote OS detection spoofing tool. It is portable and configurable, and will frustrate current state-of-the-art OS fingerprinting. This presentation will discuss the current techniques used for OS fingerprinting, and how to frustrate them. A newer version of Morph will be released with the talk, as a concrete example of the discussed techniques.

Kathy Wang broke into programming with BASIC on the Apple IIgs. She has a bachelor's and master's degree in electrical engineering from the University of Michigan, where she specialized in VLSI chip design and semiconductor device physics and fabrication. She worked at Digital as part of the Next-Generation Alpha Chip Design Team, and got to spend an entire wonderful summer blowing up Alpha chips. She has published a paper on some of the work she did there at an IEEE conference. Kathy has instructed courses ranging from Semiconductor Device Physics to Vulnerability Assessment and Penetration Testing.

Since Digital got broken up by Compaq and Intel, Kathy has focused on the software side of things. She has worked at Counterpane Internet Security, and currently works as a Senior Infosec Engineer at The MITRE Corporation. Kathy is also a founder of Syn Ack Labs, a computer security research group focused on cryptography, steganography, and low-level packet hijinks.

Toward a Private Digital Economy (Trusted Transactions In An Anonymous World)

Wavyhill
Andre Goldman

Current financial privacy tools have drawbacks arising from centralized ownership and control, and the limitations of the service-for-profit model. A better approach is to construct a fully distributed environment for economic activity which mimics in freedom and variety of action the way cash is used in the physical world.The key to this variety is the element of locale.

We introduce the 'Farmer's Market' model of anonymous commerce and refine it to a software functional description. We explore some exotic kinds of business viable in this new environment and ways to connect them to the transparent banking world.

Number theory can be used to derive an 'algebra of trust', exploited in practical ways to reduce risk in anonymous transactions, and overcome barriers to adoption of this and other digital cash systems. We also discuss the boot-strapping problem and suggest some ways to address it. Afterward, everyone is invited to participate in a role-playing simulation experiment to test the viability of these ideas using a prototype graphical software environment

Wavyhill is a software engineer having a 25 year history with industrial research organizations and developers of operating system, video, and graphics products. An anarcho-capitalist without portfolio and advocate of privacy and anonymity, he has also done experimental engineering work on artificial islands. He has no academic credentials that he will admit to.

Andre Goldman writes on law and philosophy. He works in the area of non-jurisdictional law, and was the primary author of The Common Economic Protocols.

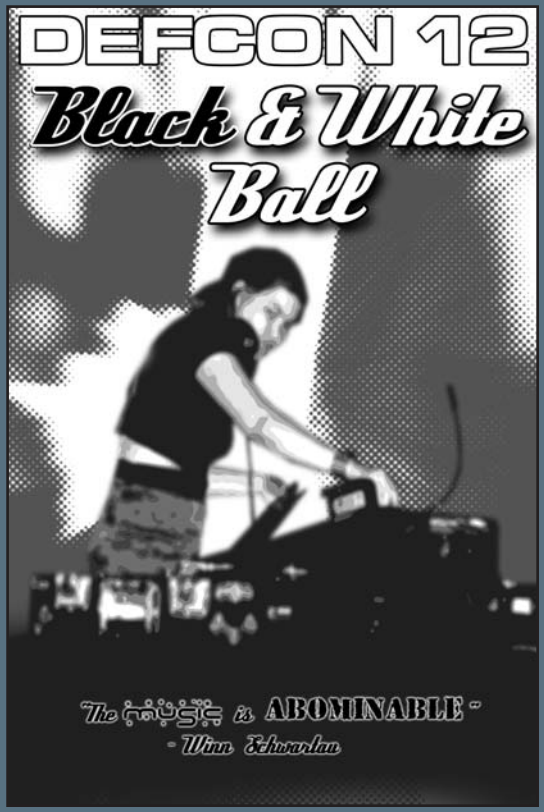
Windows Wavesec Deployment

Paul Wouters

Paul Wouters has been involved with Linux networking and security since he co-founded the Dutch ISP "Xtended Internet" back in 1996. His first article about network security was published in LinuxJournal in 1997 Since then, he has written mostly for the Dutch spin-off of the German "c't magazine", focussing on Linux, networking and the impact of the digital world on society. He has presented papers at SANS, OSA, CCC and HAL.

He is currently involved with the FreeS/WAN project, a Linux IPsec stack that aims to bring Opportunistic Encryption to everyone. For this feature, a secure DNS is needed, which triggered his interest in assisting the widespread use of DNSSEC. Wouters received his Bachelors degree in Education in 1993

DAY 1 FRIDAY JULY 30	TRACK ONE PARTHENON	TRACK TWO TENT	TRACK THREE APOLLO
11:00 - 11:50	Advanced Hardware Hacking Joe Grand	Freenet Ian Clarke	The First Inter'l Cyber War Peter Feaver & Kenneth Geers
12:00 - 12:50	Windows WaveSEC Deployment Paul Wouters	Message Security Jon Callas	Attacking Windows Mobile PDA's Seth Fogie
13:00 - 13:50		Real World Privacy n0namehere	Buffer Overflow Peter Silberman and Richard Johnson
14:00 - 14:50	Introduction to Hardware Hacking Scott Fullam	Tor Roger Dingledine	We Can Take It From Here FX & Halvar Flake
15:00 - 15:50	Bluesnarfing Adam Laurie & Martin Herfurt	Tools for Censorship Resistance Rachel Greenstadt	
16:00 - 16:50	Hack the Vote Rebecca Mercuri & Bev Harris	CryptoMail Joshua Teitelbaum and Peter Leung	Wireless Weaponry The Shmoo Group
17:00 - 17:50		Mixmaster vs. Reliable Len Sassaman	Program Semantics-Aware Intrusion Det Tzi-cker Chiueh
18:00 - 18:50	RF-ID & Smart-Labes Lukas Grunwald	Snake Oil Anonymity Nick Mathewson	VICE—Catch the Hookers! Jamie Butler
19:00 - 19:50	Weaknesses in Sat TV Protection A	Identification Evasion Adam Bresson	Bubonic Buffer Overflow spoonm & HD Moore
20:00 - 20:50	Smart Card Security h1kari	NoSEBrEaK Thorsten Holz, Maximillian Dornseif, Christian Klein	
21:00 - 22:50	Automotive Networks Nothingface	Leetest Link	TCP/IP Drinking Game



artwork by Jesse

SATURDAY • JULY 31
2100 - 0400 • APOLLO

DJ	Style	Time
wintamute/pmt munich	Electronic	22:00
Regenerator	EBM	22:45
Catharsis (EGR Records)	Hard Techno/ Industrial	23:30
Miss DJ Jackalope	Dirty Drum and Bass	00:15
Corruptdata	Electro	01:00
deaddoll	Industrial/ Dark Trance	01:45
Krisz Klink	Psytrance	02:30
psytrip	California Desert Psytrance	03:15

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 2 SATURDAY JULY 31

	TRACK ONE PARTHENON	TRACK TWO TENT	TRACK THREE APOLLO
11:00 - 11:20	DIGEX Doug Mohney	When the Tables Turn Sensepost	Mutating the Mutators Sean O'Toole
11:30 - 11:50			MySQL Passwords D. Egan
12:00 - 12:20	Digitizations And Documentary Jason Scott	Shoot the Messenger Brett Moore	The Hacker Foundation Jesse Krembs & Nicholas Farr
12:30 - 11:50			Smile, U R on Candid Camera! Kevin Mahaffey
13:00 - 13:20	Meet the Fed	Frustrating OS Fingerprinting Kathy Wang	What Do You Mean, Privacy? Sarah Gordon
12:30 - 12:50			Cracking Net2Phone Todd Moore
14:00 - 14:20	Quantum Hacking Richard Thieme	IPv6 Primer Gene Cronk	Electronic Civil Disobedience CrimethInc
14:30 - 14:50			The History of the Future Robert Morris
15:00 - 15:50	Ask EFF Annalee Newitz, Wendy Seltzer, Kevin Bankston, Seth Schoen & Jennifer Granick	Advanced Netfilter Michael Rash	This Space Left Intentionally Blank Geoffrey & Mark Farver
16:00 - 16:50		Virus, Worms and Trojans IcE tRe	Project Prometheus Grifter, Russ Rogers & Tierra
17:00 - 17:50	Down with the RIAA Nathan Hamiel	Black Ops of TCP/IP 2004 Dan Kaminsky	Kryptos Elonka Dunin
18:00 - 18:50	Hacking the Spectrum Wendy Seltzer & Seth Schoen	PDTP Tony Arcieri	Phreaking Lucky 225
19:00 - 19:50	Hacking the Media Dead Addict	Network Attack Visualization Greg Conti	Counter Intelligence/ Counter Espionage Mudge
20:00 - 20:50	Better than Life Ne0nRa1n	Toward a Private Digital Economy Wavyhill & Andre Goldman	Locking Down Apache Jay Beales
21:00 - 22:50	Movies	Leetest Link	Black & White Ball

The Ghetto Hackers are pleased to announce the Vegas 2004 Capture the Flag: Root Fu contest taking place at DEFCON 12.

Eight teams will compete for thirty-six continuous hours in a target-rich environment where the world's financial systems were written by worthless prima donnas who called in rich while the summer interns ran QA. Only offensive skills can win this game—keep your systems operational to qualify, but 0wn your adversaries to score.

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

Who is playing?

Last year's winner, Anomaly is automatically qualified to play this year's game. With the popularity of the past years games, many teams registered to play in 2004. With only seven open slots, the registered teams had to pass qualification rounds, separating the script kiddies from the truly skilled.

Teams:

1. Anomaly
2. Skewl of Rewt
3. MOCIYLB
4. Immunix
5. Enemy Combatants
6. blue9
7. Iron Grep
8. Bacon

DAY 3
SATURDAY
AUGUST 1

TRACK ONE
PARTHENON

TRACK TWO
TENT

TRACK THREE
APOLLO

	TRACK ONE PARTHENON	TRACK TWO TENT	TRACK THREE APOLLO
11:00 - 11:50	Steganography Michael T. Raggo	DMCA, Then & Now Dario D. Diaz	Hacking/Security Mac OSX Server Charles Edge
12:00 - 12:50	Subliminal Channels In Digital Signatures Seth Hardy	Google Hacking j0hnny long	The Advantages of Being an Amateur Brett Neilson
13:00 - 13:50	Hidden Data In Document Formats Maximillian Dornseif	The Insecure Workstation Deral Heiland	The Open Source Security Myth Michael Davis
14:00 - 14:50	Info Hiding in Executable Binaries Rakan El-Khalil	Old Tricks Foofus	Exploring Terminal Services Ian Vitek
15:00 - 15:50	Credit Card Networks Robert Imhoff-Dousharm and Jonathan Duncan	Blind SQL Injection Automation Cameron "nummish" Hotchkies	Digital Active Self Defense Laurent Oudot
16:00 - 16:50	Awards Ceremonies Hosted by the Dark Tangent		The DEFCON Surveys Dr. Larry Ponemon

NoteEx
Your convention, recapped

Inspired by the South By Southwest Notes Exchange your pals at VP Labs have decided to throw together one of their own. Quite simply, the DEFCON Notes Exchange exists so con attendees can swap and compare notes on talks in a central area. Drink too much the night before and miss a talk? Debating between two different speeches on two separate tracks? Check the notes exchange to see what other folks had to say about the talk you missed. Happen to take notes on something? Chip in. We operate on the zen like 7-11 policy of "Got a penny? Leave a penny. Need a penny? Take a penny." except until we get the Amazon micro payment tip jar up we'll just take your notes.
Pay a visit to DC Notes Exchange at **http://defcon.noteex.com** during or after the convention.

DEFCON on VENDORS

BAWUG
Blacklisted 411
Boblbee
Breakpoint Books
CultureJunkie
GetInsight4U
Irvine Underground
j3sus.net
MECO
Ninja Networks
No Starch Press/Last Gasp
Overdose
Rootcompromise
Shadowvex
Sound of Knowledge
tommEE Pickles
UNIX Surplus
University of Advancing Technology
Rootcompromise

Jinx: Find official DC Clothing & Merchandise at JINX Hackwear.

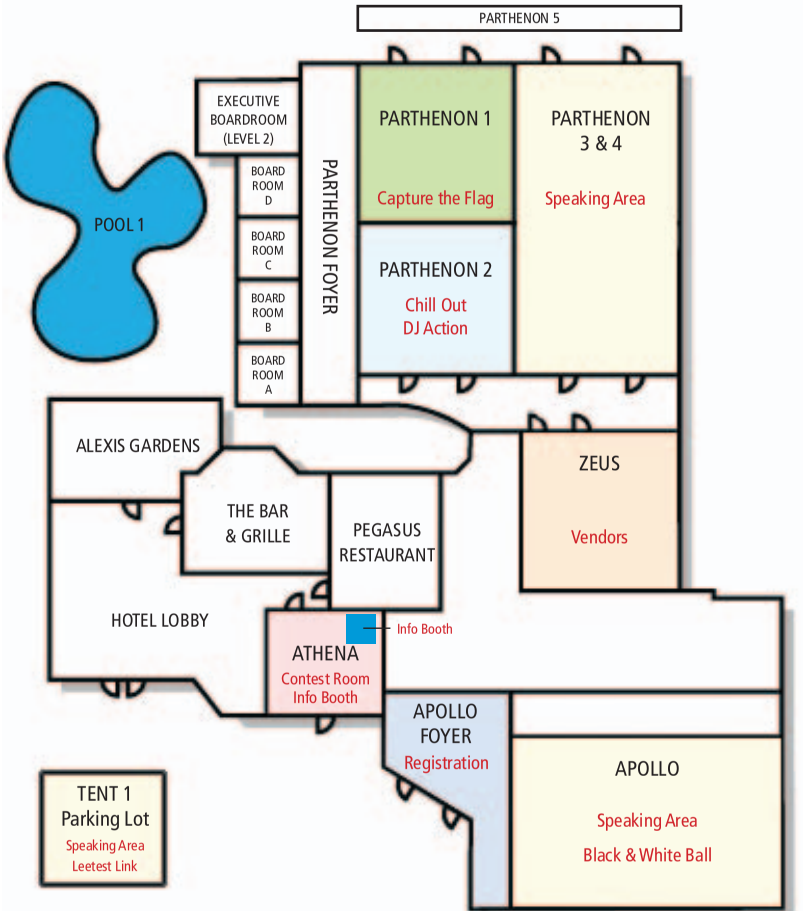
Vendors are located in Zeus.
Vendor area is open from 1000 - 2000

Sinkers to include the Dark Tangent, Jim Christy, Kingpin, DJ Jackalope, Effugas, TommEE Pickles and many more victims. Proceeds to support the EFF.

Looking for DEFCON Swag? Visit the Jinx booth and find T-shirts, cd holders, shot glasses, canteens, zippo lighters, hoodies, baseball hats, beanies, jackets, long sleeve shirts, camp shirts, playing cards, sew on patches, laptop sleeves and bags.

All official DEFCON merchandise have the DEFCON logo on them. There are 4 official t-shirt designs this year (preview them on the Winners Circle page).

DEFCON



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
Leetest Link: Tent
Movie Night: Parthenon 3 & 4
TCP/IP Drinking: Apollo
Vendors: Zeus

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

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

Shout outs to the following people, who have helped with making DEFCON 12 a reality:

Without the help of Black Beetle and Dead Addict you would not be reading this right now. Major Malfunction, Zac, Ping, TechnoWeenie, Lockheed, Cal, Bro, McNabstra, Cat Okita, Agent X, Noid, Gonzo, Josh, Skrooyoo, Spun0ut, CHS, Priest, Bink, Roamer, Xylorg, Heather G, Flea, Justabill, Pescador, Queeg, Teklord, Cyber, Stealth, Ming of Mongo, Grifter for all of his work with the 'leetest link scavenger hunt & movie channel, Monk, LRC, Xam, RussR, Saki, Zain, Shatter, Dan Dum, DevinC, JayA, Anti-Bill, Nulltone for the DEFCON Forums, tpublic for defconpics.org, Humperdink, Paul Proctor, Ray K, dedhed, Arclight, Jesse, Vandul, Timo, kampf, Joey, Scott Post, Jinx, Mark W, Charel, The Alexis Park Staff, Richard Thieme, SD, Uncle Ira's Fun Farm 'O Death, Nico, Paul Wouters, Andrew Williams and the folks at Syngress Publishing, the whole FreeBSD project, the OpenSSH and OpenSSL projects, the TOR and JAP anonominity projects.

I want to thank the support we have gotten from the scene, including the people who have made the DC Groups possible worldwide, the forum.defcon.org and forum.mydefcon.org web groups, and the defcon stuff mailing list. OK, I could go all day...

Back at DEFCON World Domination HQ we were inspired by many things. One of the largest for me has been artist Shirow Masamune, I got hooked on his art with M-66 Black Magic, and since then he has produced such works as Appleseed and Ghost in the Shell. His complicated storylines and attention to technical detail make his work a literary and art hybrid. The spin offs include the movie and TV series Ghost in the Shell and its inspired audio CDs, books, posters and the like. After a stress filled day nothing beats Motoko in GITS SAC 2 brooding in her cyber body before a little boot to the head...

Some of stuff that kept us going was every Kraftwerk title ever made. Who can't like "Machine" or "The Telephone Call"? Also Dead Addict for spinning some Manu Chao, MC Solaar, Shpongle, Infected Mushrooms, Intermix, Tricky, and Green Nuns of the Revolution, and whatever happened to be in the room that day.

For liquid fuel the drink of choice was the Mighty Mountain Dew ("A highly efficient caffeine delivery mechanism") and Fuze. For solid fuel it was Piroshky Piroshky, le Petite Cafe, Crepe de France, Local Color for their uber barista skills, Danny's Wonder Freeze, Bauhaus Coffee, Belltown Pizza, Thai Tom's, and those highly addictive Sqyntz.

Some of the client software that made DEFCON possible includes Opera & Firefox, Eudora & Thunderbird, Open Office, the Adobe Creative Suite, Real Producer, Nero, Winamp, Quark and notepad. The security tech that watches DEFCON's back includes SSH, SafeRemote, PGP, BestCrypt, F-Prot A/V, Integrity, Secure Doc, AdAware, Rainbow, and Overflow Guard. Our servers run FreeBSD and include mail by QMail, web by Publicfile, and media streaming by Real Server. That's backed up by a Sidewinder and a Cisco, a lot of time spent administering them plus a bad attitude. Hardware includes Dell, Soekris VPN cards, Palm & Nokia. Laptops include IBM, Sony, Apple, and the indestructible Amrel.

Note: After you have stumbled home, recovered from your hangover, patched all the vulnerabilities you have just learned about, restored your warez, and caught up on some sleep, please take some time and let us know what happened! Email us with evidence, links to anything con related, picture archives, stories, news articles, video, etc. We are trying to preserve our history and are looking for any and all things DEFCON.

Until next time,
The Dark Tangent