14

Haeckse

DEFCON

TABLE OF CONTENTS

	PAGE
WELCOME TO DEFCON	3
THE NETWORK @ DEFCON	4
FORUM.DEFCON.ORG	5
BEHIND THE SCENES OF THE DEFCON BADGE	6
DJ JACKALOPE	8
BLACK AND WHITE BALL	9
TCP/IP DRINKING GAME	10
AMATEUR CTF	11
TOXIC BBQ & THE SUMMIT	12
LPCON4 & DEFCON BOTS	13
SCAVENGER HUNT	14
BEVERAGE COOLING CONTRAPTION CONTEST	15
TCP/IP EMBEDDED DEVICE CONTEST	16
COFFEE WARS	17
DUNK TANK	18
SPOT THE FED	19
OTHER CONTESTS & QUEER CON	20
PRESENTATIONS	21
SLOGAN & ART CONTEST WINNERS	55
VENDORS	56
SPEAKING SCHEDULE - DAY 1	57
A NIGHT AT THE MOVIES	58
SPEAKING SCHEDULE - DAY 2	59
DEFCON MOVIE CHANNEL	60
SPEAKING SCHEDULE - DAY 3 & BOOKSIGNINGS	61
SKYBOXES	62
MAP	63
THANK YOU	BACK COVER

WELCOME TO DEFCON 14

Welcome to DEF CON 14! Holy crap, did I just say that? I've been saying that for years, but 2* this year for sure. Why?
Look around you. You are no longer in the Alexis Park, the Monte Carlo, or any other place we have held the con at before. You're at th
Riviera, new home to DEF CON! As juk8ox put it on the slogans page:
ìrsync -a -e ssh alexispark/ ‹mailto:DarkTangent@defcon.org:~/riveria/›DarkTangent@defcon.org:~/riveria/î has now been execute

As I am sure you can guess, there is a big back story to what led up to the move, but I can optimize it thus: Evolve or die. As much as I loved taking over the property, we were stagnating at the AP. With no room to grow the content or the social side of things I felt it was time to start looking for a new place. That was almost three years ago!

For this first year we get most of the meeting space, with it expanding next year by another 25% or so. So your mission this year is to learn the space, help figure out what works and doesn't as far as hang out areas, the Top of the Riv, speaking sizes, and then let us know. Just like it took a couple years to get oriented at the AP, it will take us some time now. The benefit, though, is that we can finally expand the line up of presentations and break out areas. If we play nice and don't trash the joint we have a crack at taking over the hotel down the road. Now wouldn't that be cool?

The obvious changes are that we are in a hotel with a casino. Casino == $$ == cameras == guards. Also you don't know who your neighbors are. Next year we are trying to block all of the attendees and staff on the same floors so we won't piss of the Norms, but for this year we just couldn't swing it. Oh, and no speeches on TV, for a couple of reasons. The number of channels we needed weren't available, and the entire hotel would get them. Instead we focused on getting bigger speaking areas and just transmitting DCTV and the schedule updates on our two channels.

I'm not planning on getting sued this year, so I'm really looking forward to the con. I'll check out some speeches, chill in the outside area, and find something black and shiny to wear for the B&W ball. See you there!

—the Dark Tangent DEFCON

THE NETWORK @ DEFCON

New hotel—same wireless! We're pimpin' the Aruba switches and AP's, just as we did last year.

SSID: DefCon
-[802.11a/b/g]-

Net access will be available in any of the convention areas (all speaking rooms, CTF, Vendors, Contest area, and the Top of the Riv area). We're planning some signal coverage in the main hallways, but please don't create bottlenecks by grouping up along the walls. As well we're expecting to cover the outdoor area as well, for you nuts who like to "chill" out in the heat!

Bandwidth for everyone! Last year we tripled from 1Mb to 3Mb. This year—we're bringing you 5-10Mb for your surfing pleasures!

Once again, I have to thank the crew who sacrifices their con-time in order to make all this happen: Videoman(7 yrs), Heather(5 yrs), Sqweak (2yrs), effffn (2yrs), Derek/James/Mike(Rant Radio) (3 yrs), Major Malfunction (179 yrs). Of course props to DT for hookin' us up with the Aruba gear—it's really made doing this much easier!

Cheers!
Lockheed

DefCon TV

We have two TV channels this year. Channel 27 will be our schedule & update channel. Tune in there to make sure you have the latest info on last minute schedule changes.

Channel 26 will be DCTV, but with a twist. Instead of just straight movies, we'll provide intermission material provided by YOU!

The Geek Confessions

Stop by the Info Booth, setup in the contest area. We'll have someone there who will sit down with you and videotape your own personal geek confessions. Assuming the material is "hotel safe" (and won't get you—or us—in legal trouble), we may decide to air it on DCTV for the masses to enjoy!

DefCon PhotoBlogs

Also at the Info booth we'll have a Bluetooth-equipment PC which will accept your random con-photos via Bluetooth. Those which pass the mark will make great material for DCTV. We'll post info at the Info Booth on what BT peer to send your material to.

Movies! Movies! Movies!

We'll post the schedule to Channel 27 and keep you apprised. But we know you're here for the con, not to sit around watching movies. Or are you?!

Please understand that we don't pwn this hotel—we have "normals" who will be witness to this material—you know, poor unsuspecting souls who have no idea that their family vacation coincides with DefCon. We have agreed with the hotel (in order to use their CATV system) that we will make sure all material which makes it to air is PG-rated. How "P.C.", huh?

If you see Grifter or the DC801 crew, drop 'em a thanks for providing the movie material. Same goes to the guys from Rant Radio for hookin' up all the tech to make DCTV happen!

If you have ideas ideas on how to make DCTV more fun next year, we'd love to hear it!

Email us at dctv[-at-]defconnetworking.org with your ideas!

FORUM.DEFCON.ORG

5TH YEAR ANNIVERSARY FORUM MEET
AUGUST 4 • 20:00 • SKYBOX 206

The forums will remain up during the con, so if you want to drop in and check out what others are saying and doing while at the con, it might be a good place to plan a party or tell others what they are missing!

For those of you who follow DC after the con is over on the forums, forums.defcon.org should have changed homes by now. thecotman, converge and I have been spending a lot of time getting the new machine ready and the software installed. If you check it out now it will be faster. DEF CON had to change offices, and as such is no longer sharing T1s, but has one all to itself now. We enabled http compression and moved to newer software versions on a faster box. All in all we should be good for a while!

Next up we plan to add some sort of photo system to the forums where you can upload your DEF CON related pictures, organize them, and share them with others who can rate them, etc. I want to try and preserve more of the history surrounding the con, and by getting some pictures hosted on our server we won't loose them as people change accounts, take down their old server, etc. We'll try to make a central repository. This is not to take away from the excellent work done by www.defconpics.org, but to supplement it by providing a place to host instead of an index site.

What's next for the forums? We are looking to expand it a bit by adding some more moderators and growing the content. If you haven't played around with the community calendar there yet, please check it out!

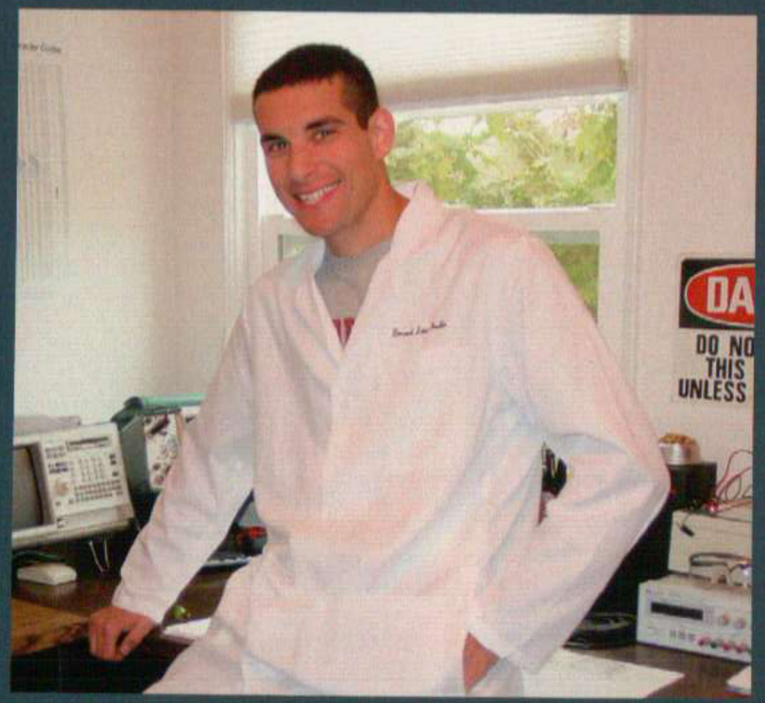
secure: https://forum.defcon.org/
normal: http://forum.defcon.org/

BEHIND THE SCENES OF THE DEFCON BADGE...

When The Dark Tangent and Ping contacted me back in February about creating a unique badge for DEFCON 14, I knew I had big shoes to fill given some of the badges from previous years. But, I couldn't refuse an opportunity to see thousands of hackers wearing something I designed. Yes, it's an ego trip—who wouldn't want to see their name in lights? Lucky for me, they had a pretty good idea of what they wanted the badge to look like and how it should function, which let us get down to business right away.

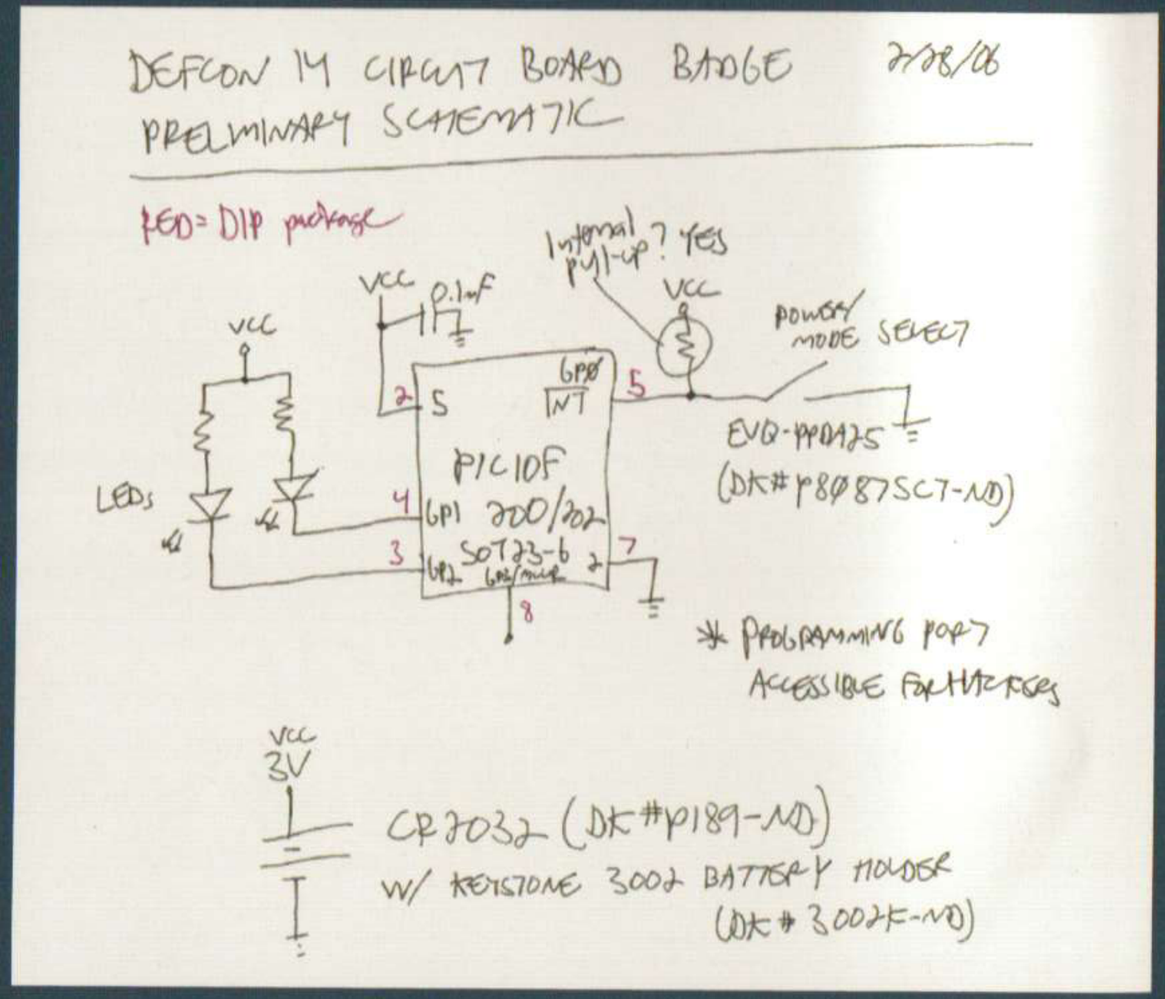
If you're up early enough and interested in details of the entire development process of the badge, from initial concept drawings to prototype electronics to completed units, and want to hear stories of the trials and tribulations that come with designing an electronic product (no matter how simple), be sure to stop by my covertly-titled "Hardware Hacking" session on Friday morning.

But, for now, here's the long, sordid tale turned short...



Joe will be giving a presentation on the highlights of the badge on Friday, August 4 at 10:00

After some conceptual sketches, physical mock-ups, and back-and-forth discussions, we had finalized the feature set and details of the artistic elements for the printed circuit board (PCB). With those locked into place, I began to sketch out the initial circuitry.



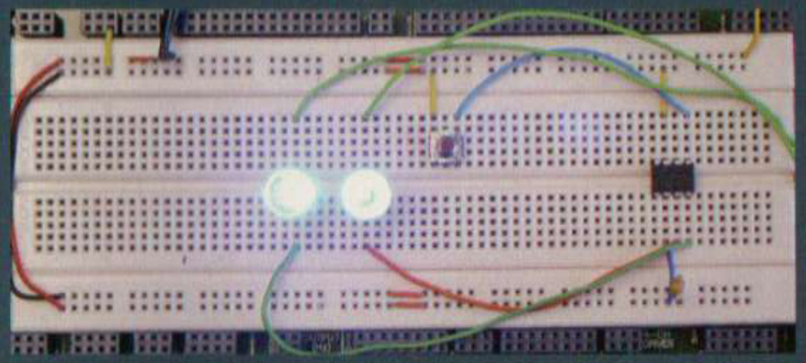
Cost was a limiting factor in choosing features and electronic components, as the badges had to come in under $5 each from soup to nuts, including all parts, PCB fabrication, assembly, and testing. I also needed to make sure that any components I selected were available in large quantities for our build of 6,055 badges and that I

A SHORT STORY

JOE GRAND (KINGPIN) • JULY 8, 2006

could obtain them in short order to start production. Flipping through the pages of the trusty Digi-Key and Mouser catalogs gave me my first draft bill-of-materials.

The next step was to turn my hand-drawn, preliminary sketch into something physical. After entering the schematic into my schematic capture package (OrCAD Capture), I built the prototype circuitry onto a breadboard and wrote the embedded code for the processor (using the CCS PCM compiler for the Microchip PIC10F202).



With the prototype properly working, I started drafting the PCB design (with Protel DXP), which was no easy feat given the specialized shape of the board based on the DEFCON logo and artistic details like the DEFCON icons on the top copper layer. Some more back-and-forth discussions with The Dark Tangent and Ping eventually yielded a final board layout.

To verify that the board functioned as expected, I ordered a few prototype PCBs from e-Teknet (after careful discussions with them to ensure that our complicated cutout areas and features were conveyed properly to their Chinese factory) and hand assembled them with a small quantity of parts ordered from Digi-Key. With The Dark Tangent and Ping satisfied with the results, I could now pull the trigger for production board and component orders.

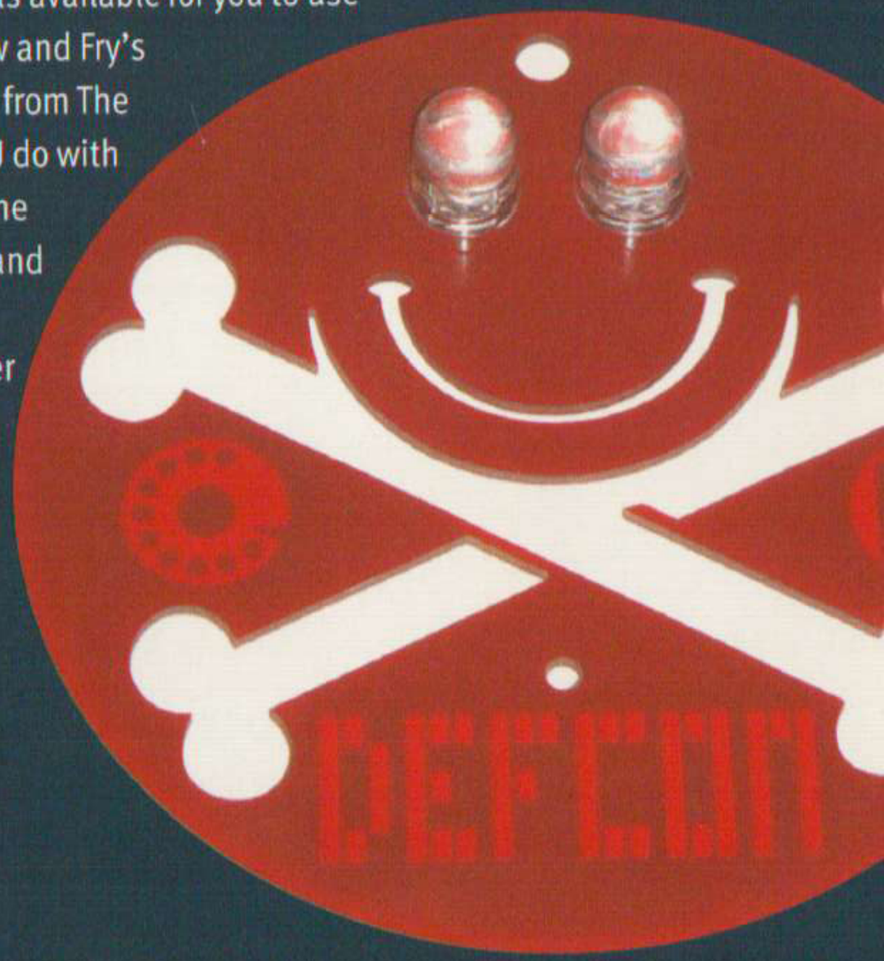
I enlisted Future Electronics to cost reduce my bill-of-materials and help with the large quantity ordering (which is significantly cheaper, but not as convenient, as ordering parts from an online distributor like Digi-Key). Unbeknownst to me, this would be the trickiest part of the process and I ran into poor customer support, misquoted lead times, and lost parts. Somehow, after laying down some pressure and being "upgraded" to a much more competent sales contact, we did end up receiving all of the components (albeit a few weeks late) and they were shipped directly to e-Teknet to handle the assembly.

At the time this article was submitted (July 8), all of the boards have been fabricated, first article assembled units have been verified and approved (in each of the seven soldermask colors), and the build is well underway. If your DEFCON badge is something other than this circuitry, then something must have gone drastically wrong!

For the dedicated hardware hackers out there, we have a challenge for you. The most obscure, obscene, mischievous, or interestingly hacked badge will be recognized and awarded at the DEFCON Award Ceremonies on Sunday. There will be some development tools available for you to use somewhere at the show and Fry's Electronics isn't too far from The Strip. So, what can YOU do with two LEDs, a switch, some discrete components, and a Microchip PIC10F202 processor? Find me over the weekend to check out what I've done to mine. Yes, even the designer gets to hack his own hardware.

Enjoy the con!

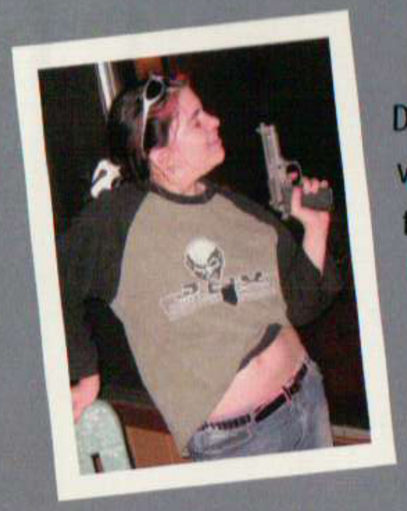
Joe



DJ JACKALOPE: OFFICIAL DC 14 DJ

"This music makes me want to kick someone's ass"

—Jimmy Palmiotti, comic book legend—



Miss Jackalope has been sending beats to Def Con and making sure that your visit to the Black and White Ball and to the pool parties has been a truly insane one. She's been here ever since the Iron Feather Journal forced her to come to Def Con and Noid gave her her spinning debut at DefCon7.



She's been playing records for 10 years and has played almost every electronic music genre you can think of. Somehow, over time, the breakbeats stuck and she stayed with jungle and electrobreaks. Her dedication to hard beats has got her opening for the likes of NYC's pH10, Ming + FS, and a variety of other DJs and live performers.



For those of you who do not live in Colorado, you are missing out on the parties she throws under the Orbis23/Colorado Pirate Coalition (www.coloradopirate.com) guises and getting to see her spin at a different venue nearly every week. She has also played at Denver's infamous Friday jungle night, Recon, and on Bass Infektion, a monthly radio show on Digitally Imported (http://www.DI.fm) hosted by DJ Tekfox. Luckily for those of you here, she will be spinning at the Black and White Ball and anywhere else that will allow her to at Defcon14.

DJ Jackalope's website is located at: http://www.dj-jackalope.com, she has a little grey cat, and she also has an army.



THE NEW TWO NIGHT

BLACK & WHITE BALL

TOP OF THE RIVIERA BALLROOM IN THE
MONACO TOWER ON THE 24TH FLOOR
FRIDAY & SATURDAY • 20:00 - DAWN

FRIDAY NIGHT (THE BLACK BALL)

Brought to you by Kontrol Faktory's Mike Hell and Krisz Klink.

Release the deviants for an evening of darkwave, industrial, EBM, and if you're found deserving, a Blackout Party.

Krisz Klink (spinning old school Industrial)
DJ Shatter
DJ Delchi
DJ Spekulum

Recommended Attire: Blacks, leather, bondage gear.
We will be bouncing people who don't make an effort.
No, there is no "tee shirt and hat" look.

SATURDAY NIGHT (THE WHITE BALL)

All your tried and true electronica, trance, and drum and bass DJs and ban
from past Defcons that weren't afraid to return for more punishment.

Featuring a special appearance by the Minibosses.

Catharsis
DJ Casey
Mindpop
Ms DJ Jackalope
Regenerator
The Minibosses
wintamute/pmt

Recommended Attire: Whites, costumes, full feathers

ORGANIZED BY BINK

TCP/IP DRINKING GAME

HOSTED BY MUDGE ON FRIDAY • AUGUST 4 @ 21:00

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

For this game you will need:

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



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

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

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

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

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

This is the first stage of the game. In later stages of the game the panel or panelist can negate drinks that are accrued in the question. If the panelist were to answer the previous question with something along the lines of: A: Having the SYN, FIN, ACK, URG, and PUSH flags set in a TCP packet is often referred to as a Christmas Tree Packet. However, it would be more appropriate to include the two reserved flags for explicit congestion notification in addition: ECN-Echo, and CWR (congestion window reduced).

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

It starts going down-hill from here...

AMATEUR CTF

King of the hill is a simple game, take the hill, keep the hill, for as long as possible. Who ever can do that the longest wins, its that simple. There are 10 computers or "victims" on the network, along with a scorekeeper and a dhcp server. Each of these 10 computers are vunarable to SOME sort of attack. Some are easy, some are a little harder, there level of difficulty is ranged from 1 - 10, 1 being the easiest to hack and 10 being the hardest. Hack a service on any box and you get points, keep control of the box without stopping any of the services or rebooting the box and you will get more points. who ever has the most points at the end of the game wins.

Last year, we had one server which was the hill. It was running Mandrake 2005 LE with all services running and no firewall. The scorekeeper polled certain services every minute to see who's team name was in the banner, and recorded that. As it turns out, nobody was able to put their team name into any of the banners. About 2/3 of the code for the scorekeep was written the night before the con, and we didnt' get a chance to test to see what hacks worked.

That's where this year will be different...

First of all, we'll have tested vulnerabilities. This will prevent the "no winner" syndrome that we were infected with last year. Also, we're going to have 10 servers to take over. Each one will be bigger and tougher than the previous, and the rewards will reflect this. A service on victim #1 will score 1 point per minute, victim 5 will be 5 points per minute and so on up to victim #10. The scorekeeper will be very much like last year, however we decided to make it a little more interesting. We're not going to tell you what services we're monitoring. We're specifically tracking down hubs for this contest and not switches, so if you want to know what files we're monitoring and how we're monitoring them you'll have to figure it out.

I will say that the basic pricipal will be the same, the scorekeep will look to see what's in a certain file and make a note of it. On lower levels this may be as simple as just a team name, but on the upper levels there may be some encoding or even encrypting!



ORGANIZED BY VYRUS & DC949

TOXIC BBQ

The BBQ, like Defcon, has been cancelled ...due to rain? HAH! TBBQ3 is happening, RAIN, SHINE, SLEET or PLAGUE. *You* may opt for rumors of cancellation again this year, but we will be out making the best of whatever Vegas has to offer. Full swing folks, brings your meats, breads, sauces, drinks and overall BBQ leetness. The pre-bbq will be fully reinstated this year, taking over the nearest Sam's by storm. The Unofficial Defcon 14 Toxic BBQ is back.

Just to be completely, absolutely, and quite redundantly clear; rain will not stop the TBBQ. Show up for a good time.

When: Thursday, August 3rd 18:00:00 until the event dies out
Where: Sunset Park



THE SUMMIT 2006

2nd annual EFF fundraiser sponsored by local Las Vegas hackers.

When: Thursday Aug 3, 2006
Time: 9:00 PM - 12:00 AM (midnight)
Where: TBA
Cost: $35 @ door
Ticket Limit: 200 people max
Web Site: http://www.vegassummit.org

theSummit puts togeather EFF, Black Hat / Defcon speakers and Security Experts from around the world. We then open the doors for you to come and hang out with them, pick their brains or just buy em a drink! By only selling small amount of tickets and renting a small location you get an intimate environment to hang out with experts in the online rights and computer security industry.

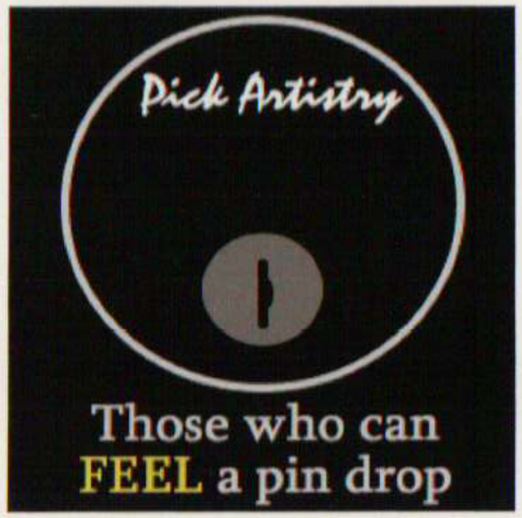
Last year we were able to raise approx $4,200 for the EFF! Hopefully we can beat that number this year!

LPCON4

The Lock Picking Contest is back!!! LPCON4 will be composed of two primary events: The timed Lock Picking Contest and the Lock Picking Village.

The timed event will be composed of three elimination rounds consisting of multiple 6-contestant heats over two days. The final event will be a competition among the 4 fastest times and will be done on the now infamous "Tower of Terror".

The second event is the Lock Picking Village. Here you will earn points based on different locks that you pick in the Lock Picking Village. Some will be easy, some hard and the lock picking team will track your scores throughout DEFCON with a prize awarded to the top point getter. You can only get points for each lock once. We are planning for demos, demonstrations, discussions and some other fun activities.



http://www.securitytribe.com/~doc/lpcon4.

ORGANIZED BY DOC



The objective of the DefconBots contest is to build a computer controlled airsoft gun which can shoot down targets. No human control is allowed, it has to be 100% autonomous. Building the hardware is easy this time, the software will separate the winners from the losers.



http://defconbots.org



ORGANIZED BY KALLAHAR

SCAVENGER HUNT

So you think a scavenger hunt is just a game for girlscouts? You think that you have the skills to stake your good name on the line and compete? Are you looking to get rid of that extra self-respect you have laying around? Then we welcome you to the rebirth of the scavenger hunt... DefCon style!

Looking for a game that will challenge every ounce of your leetness?

You've come to the right place.

The rules are the same as they have always been:

1. 5 players to a team max
2. You must submit the "item" to an OFFICIAL member of the ScavengerHunt staff. You will be able to identify these fine people by the nifty ScavHunt badge that they will be wearing.
3. Only one "item" per team will be counted and you must present "proof" to an Official Judge (see rule #2). Sometimes that proof will be photos and sometimes it will be video. Sometimes it may entail you preforming some sort of action and sometimes it will entail you making someone or something else do something... ya never know.
4. HackerHouse.org owns all media generated by the scavenger hunt and may publish it as they deem fit. (we wont send anything to your mom)
5. Bonus items are high point bonus endeavors that you get from Official Scavenger Hunt Judges (again, see Rule #2) after having turned in another item. Not all items on the list have bonus items attached to them, but all teams will be given the same bonus item after having completed each specific item on the list (that will not be reviled until someone has turned in said item and received the bonus)
6. The first team to submit an item will be awarded a bonus 5 points.
7. The team with the most points by noon on Sunday wins. The official list will be released on Friday, the game begins then.

But don't fret, in the past there have been one man teams that have only competed for a day and still walked away with a sizable amount of points. This year there will also be a publicly known bonus of getting other teams to play. Think of it as some sort of sadistic MLM... you sponsor another team and you get points.

www.HackerHouse.org/Hunt

ORGANIZED BY SIVIAK

BEVERAGE COOLING CONTRAPTION CONTEST

This contest was a BLAST last year. In the past, there were two categories of competition: All contestants will be tested on cooling a beverage which had been opened and poured out of its original can and (ultimately) into a glass. All participants will be given an open beverage can and will be expected to pour the contents into their cooling device.

There will be plenty of free beverages available for participants to, ahem, "calibrate their equipment" and so forth. C'mon, it'll be fun... why not give it a try?

Friday, August 4, Noon.
Outdoor Area.

http://deviating.net/bccc/







ORGANIZED BY DEVIANT OLLAM

TCP/IP EMBEDDED DEVICE CONTEST

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

There are two categories of devices in this contest:

- The first category is TCP/IP embedded devices.
- These are stand alone devices which simply need to be plugged into a hub or switch. The device must host a TCP/IP aware service which someone can control and/or query a status from over a LAN or the internet and have it report back to the remote client that is controlling/querying it.
- The second category is TCP/IP enabled peripherals.
- These are devices which must be connected to a host system such as a laptop or desktop computer which hosts the TCP/IP enabled service for the device. The host system must be able to communicate with the attached device in order to control it and/or query its status over a LAN or the internet and report back to the remote client which is controlling/querying it.
- Devices in each category will be judged on originality, functionality, best value for actual cost and the coolness factor.

Three main awards will be available. One for Best TCP/IP embedded device, Best TCP/IP enabled peripheral, and the Haxor's Choice Award where your peers vote for what they think is the most uber elite device in the entire contest. Be sure to expect some extra goodies for participating.



ORGANIZED BY DC 480

COFFEEWARS

Friday, August 4th. 10:00 AM. Entries can arrive any time after 9:00 AM.
Brewing starts at 10 promptly. Coffee Wars usually ends about 11:00 AM.

Wake up and smell the coffee war, people: DefCon 14 is here and that means anothetition.

What could be more fun than the start of DefCon? Starting DefCon with a bloodstreaer edition—the seventh—of the world's best-known hacker coffee compm full of psychoactive chemicals, that's what! But which chemicals, and how to get them there? Allow us to offer a suggestion: caffeine is a pretty good one, and coffee is an excellent medium for delivery. OK, we know that's not exactly a novel concept. Moreover, we know that hackers hate inferior solutions (get it?), and so we arrive at a critical question: which coffee is the best?

Good news! We've assembled an enthusiastic team of experts to find the answer. For the seventh year in a row, we will gather at the start of DefCon to conduct CoffeeWars, the craziest and most useful competition of them all. First, we invite coffee-loving hackers to submit their favorite beans for competition. The good stuff: whole beans, unflavored, from your favorite roaster. The contest staff sets up a blind taste test with a standard set of brewing tools and methods, and our esteemed judges sample and rate each brew. We tabulate the results, and the winner is announced at the closing ceremony, with the appropriate degree of glory and spectacle.

Why do we go to such lengths? Why do the judges punish their nervous and renal systems to such a degree? Why do we cart a truckload of supplies to Las Freaking Vegas every summer? Make no mistake: it is all about love. Love of coffee, to be sure, but also love for our fellow hackers. We want to make sure that you have access to trustworthy, impartial information about the things that are important.

We don't want you to spend the whole year wondering where the good coffee is. We don't want you to run the risk of buying horrible inferior coffee. That's why, each and every damn year, we publish all our results in full.

Our process is simple:

Grind --> Brew --> Drink --> Vote

But our goal is lofty: to discover and honor the coffee that hackers love best. If you visit us, you'll find us hard at work, throwing ourselves headlong into the coffee war. If you bring your beans, we will greet you with respect, and subject them to our rigorous tests. But who knows? Maybe yours will be the batch favored above all others. Victors in prior coffee wars have gone on to become world leaders, prizewinning scientists, and reclusive billionaires. These last assertions are slight exaggerations, but it should nevertheless be clear that having entered coffee wars is a badge of honor, and that winning cannot possibly fail to make you more popular.

Plus, I bet it looks good on the resume, if you're into that kind of thing.

www.coffeewars.org

ORGANIZED BY FOOFUS & SHRDLU

DUNK TANK

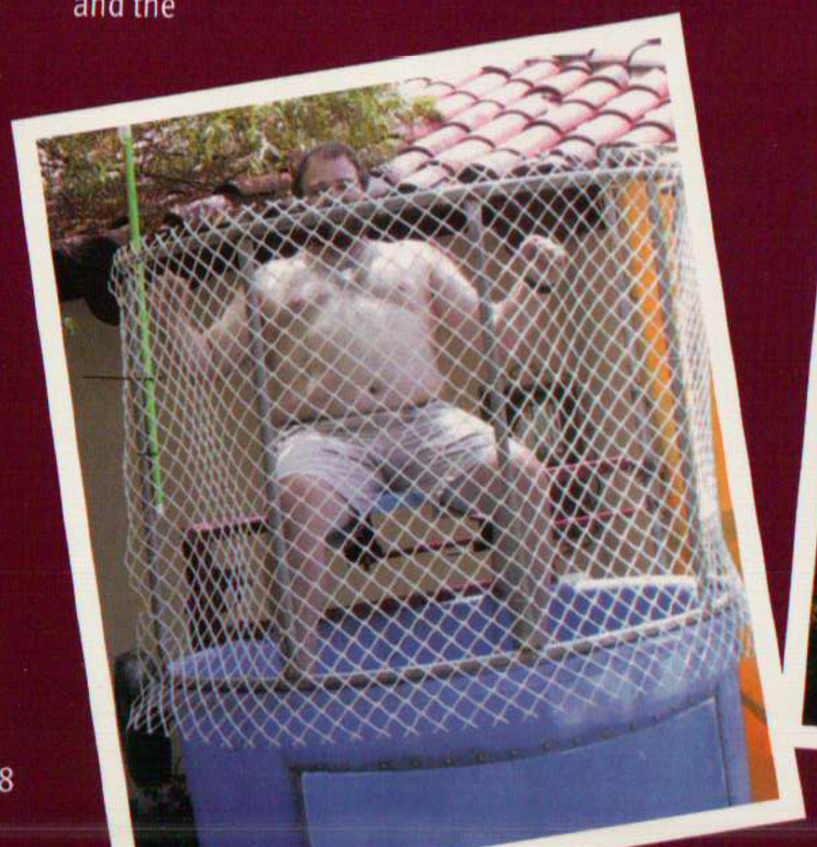
WHEN: FRIDAY AND SATURDAY, ALL DAY • OUTDOOR AREA
RUN BY ERICH AND MEL

The dunk tank is a fundraiser for the Electronic Frontier Foundation (EFF).

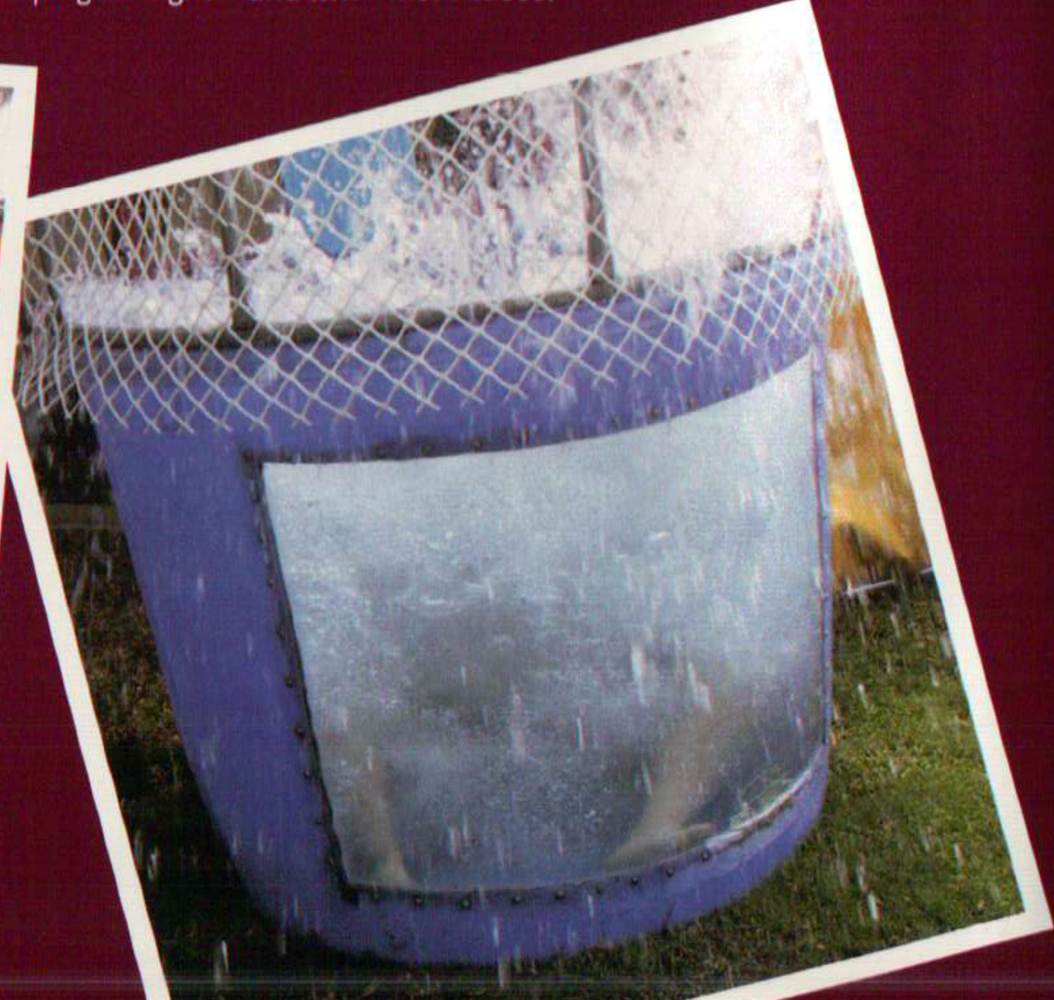
About the EFF: From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense. EFF broke new ground when it was founded in 1990—well before the Internet was on most people's radar—and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights.

Blending the expertise of lawyers, policy analysts, activists, and technologists, EFF achieves significant victories on behalf of consumers and the general public. EFF fights for freedom primarily in the courts, bringing and defending lawsuits even when that means taking on the US government or large corporations. By mobilizing more than 50,000 concerned citizens through our Action Center, EFF beats back bad legislation. In addition to advising policymakers, EFF educates the press and public. Sometimes just defending technologies isn't enough, so EFF also supports the development of freedom-enhancing inventions.

EFF is a donor-funded nonprofit and depends on your support to continue successfully defending your digital rights. Litigation is particularly expensive; because two-thirds of our budget comes from individual donors, every contribution is critical to helping EFF fight —and win—more cases.







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.

OTHER CONTESTS

CAPTURE THE FLAG

who: organized by Kenshoto
when: Friday 10:00 - Saturday midnight
where: Royale Pavilion 3-4

HACKER JEOPARDY

who: organized by Winn Schwartau and Nick Farr
when: Friday & Saturday at 21:00
where: Royale Pavilion 1-2

NETWORK APPLIANCE CHALLENGE

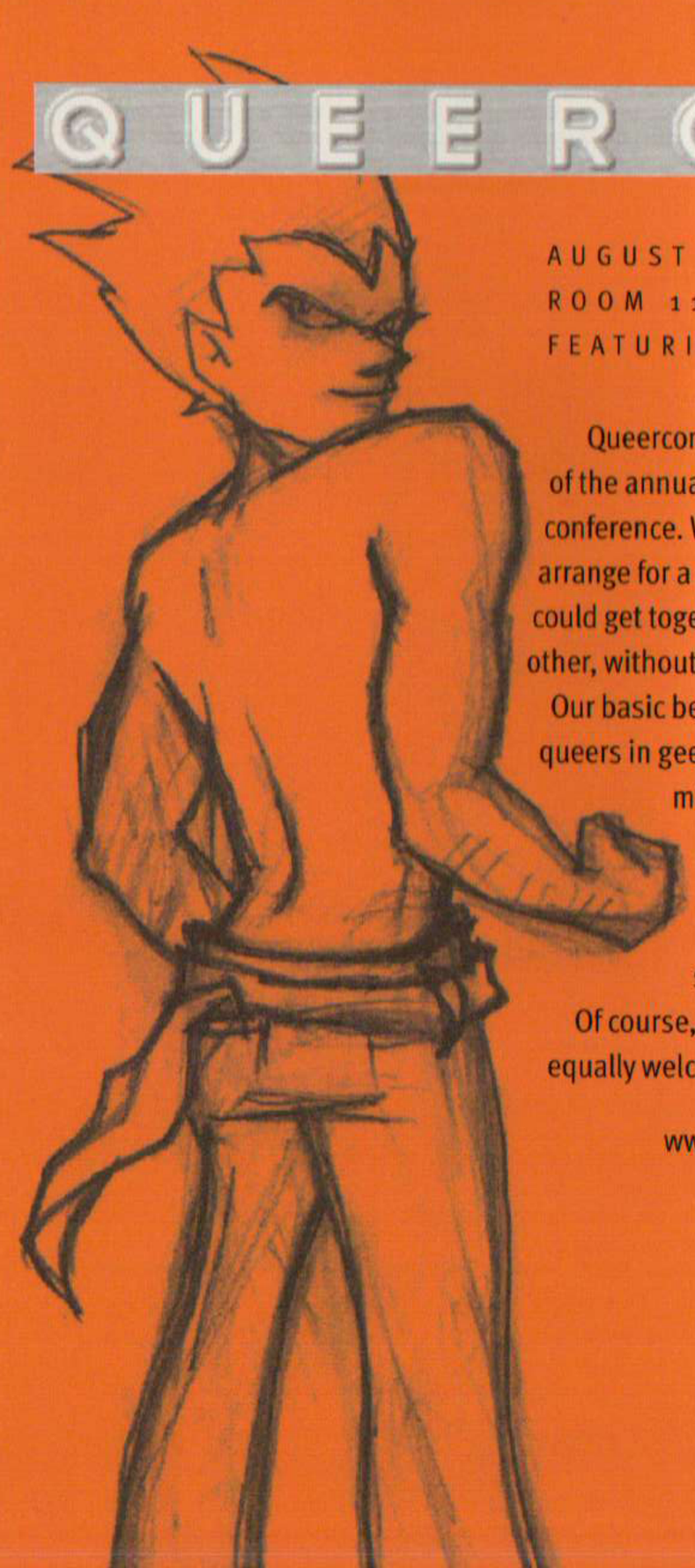
who: LosTboy and Neural
when: TBD
where: Contest Area

LoST'S @ CON SUB-CHALLENGE

who: LosTboy
when: starts Friday until solved
where: Contest Area

WARDRIVING

who: Thorn
when: starts Friday
where: Contest Area



QUEERCON

AUGUST 4 • 21:00 •
ROOM 114/115
FEATURING DJ CMOS

Queercon is a hacker party inside of the annual Defcon hacker conference. We decided to try and arrange for a way that queer hackers could get together and meet each other, without any fear of predjudice. Our basic belief is that there's more queers in geekdom than most people might think, so if we can meet a few of them, maybe make a few new friends, that sounds sweet to us.

Of course, anyone queer-friendly is equally welcome, and cheers to you.

www.queercon.org

PRESENTATIONS

COMPLETE PRESENTER BIOS & PRESENTATIONS MAY BE FOUND ON THE DEFCON.ORG WEBSITE

The Making of atlas: Kiddie to Hacker in 5 Sleepless Nights

atlas

atlas was just a kiddie when asked to write his first exploit in order to qualify for dc13's capture-the-flag. After conquering his sense of inadaquacy, he went on to win the individual competitiion and finish third even among the teams. This presentation will introduce you to atlas, to hacking, and to the pivotal "Stage 3 Binary" which turned the man's life upside down. The talk will be an entertaining walk through his efforts to understand and write a network exploit, some of his lessons learned, and some tools which made hacking a bit easier. The talk will include use of GNU Debugger (gdb), objdump output, ReadElf, Ktrace, and the @ Utility Belt toolkit (newly released).

People who will find this talk of interest include:

- Noob hackers with an interest in writing exploits
- Anyone interested in the defcon CTF drama
- Friends of atlas who wish to heckle and otherwise find amusement at his expense

atlas, *a disciple of the illustrious Skodo, has a history in programming, systems support, telecom, security, and reverse engineering. His introduction to the hard-core hacking world was through dc13's CTF Qualifiers. atlas went on to win the individual contest and place third overall. atlas has written the WEP-cracking tool bssid-flatten and the @ Utility Belt toolkit.*

Discovering Mac OS X Weaknesses and Fixing Them with the New Bastille OS X Port

Jay Beale, Lead Developer, Bastille Linux

The Mac OS X operating system is beautiful, but it's not as secure as you think. It's mostly Unix under that shiny GUI and while we've come to expect a very locked down system from recent Unix/Linux releases, that expectation isn't entirely realistic when it comes to OS X. For instance, the firewall GUI tool makes it seem like you can create a default-deny firewall that only lets packets from established sessions in. The firewall it produces, though, is full of holes! Whatever you do, don't take your OS X laptop onto the wireless network here! Write your own replacement or take the one we'll offer in this talk, where we'll introduce the new OS X port of the popular Bastille Linux system lockdown and audit tool, Bastille OS X.

Bastille increases the security of OS X systems. It starts by building a real firewall configuration that you can tune to your needs. It continues by deactivating services like the information-leaking Bonjour service, which a remote attacker can use to get your Security Update (patch bundle) level, hardware versions and machine name. Finally, it configures the remaining operating system components, doing things like isolating local users from the service that gives them the length of all users' passwords. There's a lot more than that, though. Come learn about OS X security, learn how to harden and see the newest part of the Bastille family: Bastille OS X!

Jay Beale *is a information security specialist, well known for his work on mitigation technology, specifically in the form of operating system and application hardening. He's written two of the most popular tools in this space: Bastille Linux, a system lockdown and audit tool that introduced a vital security training component, and the Center for Internet Security's Unix Scoring Tool. He also focuses his energies on the OVAL project, where he*

works with government and industry to standardize and improve the field of vulnerability assessment. Jay is also a member of the Honeynet Project, working on tool development.

Jay makes his living as a security consultant with the firm Intelguardians, which he co-founded. Prior to consulting, Jay served as the Security Team Director for MandrakeSoft, helping set company strategy, design security products, and pushing security into the third largest retail Linux distribution.

Phishing, it starts with "Ph" for a reason. Some best practices to detect and prevent for some new point of attack methods

Teli Brown, Brown Communications Security Consulting, Secure Science Corporation

Phishing, it starts with "Ph" for a reason. Some best practices to detect and prevent for some new point of attack methods.

When banks and other financial institutions tell their customers to only give personal information (e.g.: Credit Card, Social Security Number, ETC) via the telephone, because of online attacks from phishers, that's when phishers get creative and go back to what the root of phishing has been and blend it with some new technologies.

***Teli Brown** has done Security consulting for major telecommunications companies, aiding in tracking terrorist and malicious telephone users. He has also done massive amounts of testing with number delivery in SS7, and was able to identify and backtrace the flaw in SS7 that allowed people the ability to change their "Charge Number". Now spends his time consulting for small businesses for voice services.*

Exploit Writing Using Injectable Virtual Machines

Wes Brown, Founder, Ephemeral Security
Scott Dunlop, Developer, Ephemeral Security

Mosquito is a secure remote execution framework available via LGPL that combines high-grade cryptography and a small efficient virtual machine on both ends to ensure that intellectual property is protected. It also presents a dynamic environment on a target host that can be reprogrammed on the fly over a secure communications channel to fit the current situation.

The virtual machine was written from scratch for this purpose, with a built in cryptography library, and was optimized for size with an eye towards being able to inject it. The virtual machine's native programming environment is a Scheme-derived Lisp-family language, with an optimizing bytecode compiler. It is also cross-platform using ANSI C and GCC, currently running on OpenBSD, Darwin, Linux, and Win32. Compiled bytecode is portable between these platforms, much like Java except it fits within 150K on
some platforms.

This talk will demonstrate the use of Mosquito to write exploits on the fly while the audience watches; the advantages and flexibility of using a virtual machine will be leveraged to implement a second stage puddle-hop exploit into another host. The cross-platform advantages of writing exploits in a portable virtual machine will also be demonstrated. There will be some discussion of Mosquito itself to give context and understanding.

***Wes Brown** is a long-time network security practitioner who specializes in code reviews, web application assessments, penetration testing, and tools development.*

In founding Ephemeral Security, Wes hopes to advance the state of the art in network security by doing innovative and original research work. When not conducting consulting work, he has spent the last year and half on the Mosquito Environment along with other members of his company.

Fun with 802.11 Device Drivers

Johnny Cache

The 802.11 link-layer wireless protocol is widely known for its design flaws. Unauthenticated management packets, a ridiculous attempt at providing link layer confidentiality and authentication (WEP), and general vendor stupidity have all contributed to 802.11 being the most sensationalized protocol ever mentioned in the media.

All of the above topics have been beaten to death. Instead this talk explores new advances not in design problems in 802.11, but in implementation issues. The two major advances in 802.11 security will be covered, device driver vulnerabilities and link layer fingerprinting techniques. 802.11 fingerprinting represents the first time that a link-layer protocol has been vulnerable to finger-printing attacks. These attacks can provide useful information to the attacker, allowing him to accurately target the latest weapon in any wireless hackers arsenal: 802.11 device driver exploits.

Johnny Cache *is responsible for many wireless hacking tools. These include jc-wepcrack (a distributed wep-cracker) jc-aircrack (a complete aircrack re-write in C++), and also helped h1kari create pico-wepcrack (a FPGA accelerated WEP brute forcer). Cache is currently pursuing his Master's degree in computer security. He is also co-author of "Hacking Exposed Wireless". His latest accomplishments can be found in Airbase, available at www.802.11mercenary.net*

Hacking FedEx Kinko's: How Not To Implement Stored-Value Card Systems
Strom Carlson, Hardware Security, Researcher, Secure Science Corporation

ExpressPay is a stored-value cash card system which utilizes the Infineon SLE4442 chip; it was developed by enTrac Technologies of Toronto, Ontario, and its largest application is as the pre-paid cash card system in use at FedEx Kinko's. Analysis of a few dozen cards reveals that the data stored on the card is unencrypted and poorly protected against fraud, and a simple attack can be used to obtain the security code necessary to alter the data on the card. This talk will step the audience through the analysis, research, attack, and subsequent tests performed on the ExpressPay system, and conclude with recommendations on how to implement a more secure stored-value card system.

Strom Carlson *is a hardware security researcher at Secure Science Corporation, the organizer of the Los Angeles area Defcon Groups chapter (DC213), and the co-host of Binary Revolution Radio. He enjoys tinkering with technology, playing with telephones, and having a good time with whatever he happens to be involved in.*

SOCIAL MESSAGE RELAY: Using existing social networks to transmit covert messages in public
Strom Carlson, Hardware Security, Researcher, Secure Science Corporation
skrooyoo
datagram
Vidiot

In the age of NSA phone taps, mandatory data retention, CALEA, the PATRIOT Act, and national firewalls, establishing a truly covert communications channel without leaving a trail is becoming almost impossible. Even when strong encryption is used to protect the message, Government agencies now have the ability to use pattern analysis to pinpoint almost all participants in the conversation. Without tremendous diligence, truly anonymous communication is almost impossible.

But what if you could skip having to create the communications channel entirely? What if you could have unwitting, or even willing, third parties spread your message for you? The larger the network of people spreading the message, the more difficult traffic analysis becomes as the signal-to-noise ratio increases. Convenient anonymity for the sender and recipient of the message becomes possible again.

The presenters will demonstrate how they were able to create a publicly available communications channel and use thousands of unwitting participants to spread their encrypted messages. The presentation will also include speculations on how to create networks designed to foil traffic analysis attempts, and observations about the culture of the online cryptographic community, and the nature of collaborative problem solving.

Legal Aspects of Computer Self-Defense and Aggressive Self-Defense
Robert W. Clark, Command Judge Advocate, 1st Information Operations Command (ACERT Legal Advisor) U.S. Army

This presentation looks at several scenarios of aggressive self defense. It applies the law to each of the participants in various schemes—to the aggressor and to the defender. We see where simple self defense options could actually result in prosecution to the aggressor; prosecution of the defender; prosecution of both; or, be faulted for

screwing up an investigation rendering a prosecution impossible. Many of the legal rationales for aggressive self defense will be discussed from the typical discussion of self defense to the law of nuisance and self help. This presentation seeks to simplify the aspects of aggressive and non-aggressive self defense.

Major Robert Clark *is the Command Judge Advocate for the Army' 1st Information Operations Command. As the sole legal advisor, his primary duty is to advise the Army's Computer Network Operations Division on all aspect of computer operations and security. This role has him consulting with the DoD Office of General Counsel, NSA, and DoJ Computer Crime and Intellectual Property Section. He lectures at the Army's Intelligence Law Conference and at the DoD's Cybercrimes Conference.*

Legal Aspects of Internet & Computer Network Defense - A Year in Review
Computer and Internet Security Law 2005-2006
Robert W. Clark, Command Judge Advocate, 1st Information Operations Command (ACERT Legal Advisor) U.S. Army

This presentation looks at computer network defense and the legal cases of the last year that affect internet and computer security. This presentation clearly and simply explains (in non-legal terms) the legal foundations available to users and service providers to defend their networks. Quickly tracing the legal origins from early property common-law doctrine into today's statutes and then moving into recent court cases and battles. We will look at the past criminal prosecutions and precedents, both civil and criminal, since we last met a year ago. As always, this presentation will quickly become an open forum for questions and debate.

Googling: I'm Feeling (un)Lucky
Greg Conti, United States Military Academy

Birth, School, Work, Death. Imagine every web search you,ve ever done placed on a timeline of your life. Is there anything on that list you wouldn,t want your mother (or employer) to know about? How about the aggregate web searches of your entire company? What if they fell into the hands of a competitor? Recent trends indicate that we can no longer rely on the privacy policies of individual web companies to keep this information private. In this talk, we'll examine the many ways we disclose information in return for free web services as well as how effective you think your privacy countermeasures are. This session won't be a monolog, but an active discussion on the problem of web-based information disclosure. As part of the talk, I'm releasing a program that will extract web searches from your Firefox browser's cache to show you what you,ve been disclosing.

Greg Conti *is an Assistant Professor of Computer Science at the United States Military Academy. He holds a PhD in Computer Science from Georgia Tech and a Bachelor of Science in Computer Science from the United States Military Academy. His areas of expertise include network security, information visualization and information warfare.*

The Evolving Art of Fuzzing
Jared DeMott, Vulnerability Researcher, Applied Security, Inc.

The Evolving Art of Fuzzing will be a technical talk detailing the current state of fuzzing and describing cutting edge techniques. Fuzzer types, metrics, and future research will be presented. Also, three of ASI's private fuzzer tools will be discussed. They will be released on the DEFCON CD.

Jared DeMott *is a vulnerability researcher for Applied Security, Inc. (ASI). Jared earned a masters degree from Johns Hopkins University and is currently pursuing a PhD from Michigan State University, with dissertation work to be done on fuzzing.*

FEAR!(?) The Census Bureau
Steve Dunker

The Census Bureau is the Only Federal Agency that is acquiring detailed personal data on Every person in the United States. While the Census provides valuable information that is vital to our form of government, major privacy concerns exists. The potential for abuse of the data has historical roots, the most notorious being the rounding up and relocation of Japanese-Americans during World War II.

Learn how the Social, Economic, Housing, and Financial characteristics being gathered can be legally used against you. We will examine how dangerous the data could be if it was used illegally. (If you are paranoid, you do not want to miss this!)

Finally, we will examine the laws that mandate that every American must cooperate with the Census Bureau or face possible Civil and/or Criminal Punishment. What are your options when that Census worker shows up at your door and threatens you with prosecution by the U.S. Attorneys office?

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

SAMAEL (Secure, Anonymous, Megalomaniacal, Autonomous, Encrypting Linux) and NARC (Network Analysis Reporting Console).

dr.kaos (aka Taylor Banks), Founder, kaos.theory/security.research
arcon (aka Adam Bregenzer)
atlas (aka Gavin Mead)
beth (aka Beth Milliken)
digunix (aka Kevin Miller)

From the 1337 haxors that brought you Anonym.OS, kaos.theory/security.research presents SAMAEL (Secure, Anonymous, Megalomaniacal, Autonomous, Encrypting Linux), the natural evolution of our secure, automagicically anonymizing operating system, Anonym.OS into a kick-ass anonymizing server!

When kaos.theory released the Anonym.OS at ShmooCon in January of this year, we received many requests for features we had already planned to implement: media players, smaller distribution size, office suites, better speed, USB functionality, etc. "Sure," we collectively replied, "we'll get right on that."

But we didn't. We tried, but we realized that maintenance releases aren't 1337. Instead, we're back to release SAMAEL, a blackbox gateway that creates -- in a few simple steps -- a secure, anonymizing, transparent firewall and proxy server, protecting its users' love of sex, drugs, and rock and roll from embarrassing public disclosure (even better than the Kennedys).

Making use of Gentoo, Transocks, Tor, and sweet, sweet Python, SAMAEL provides all of the services expected in a modern Linux firewall, including DHCP, a Captive Portal, and Web-Based Administration! The guiding principle of Anonym.OS and its derivative projects has remained "Anonymity for Everyone;" kaos.theory's SAMAEL takes that motto to the next level.

But there's one more thing. And it doesn't involve sweatshop labor or black turtlenecks.

Getting useful, attractive reports out of scanning tools is a bitch. People pay vendors thousands just for some slick charts and graphs. Why? Because SQL is hard for a boot-camp MCSE. So get your 'Security for Dummies' books and your free Nessus downloads ready, folks, because we've got scripts and queries all packaged up as pretty as your mom on a Friday night. kaos.theory's newest member, jonathan white, joins atlas and crew to introduce NARC, the Network Analysis Reporting Console.

In its initial release, NARC can utilize output from common security tools like Nessus, Paros, and NMap to populate a database via automated scripts for reporting purposes. Version 0.DC14 also includes rudimentary reporting capabilities.

***Taylor Banks (aka dr.kaos)** has written and delivered training and provided security consultation to thousands of security engineers, architects, managers and executives from hundreds of organizations including Bristol-Myers Squibb, Ernst and Young, FedEx, IBM Global Services, PricewaterhouseCoopers, and VeriSign as well as the US Department of Defense, Federal Bureau of Investigation, the US Marine Corps Computer Emergency Response Team (MARCERT) and the National Security Agency.*

***Adam Bregenzer (aka arcon)** has been working in the IT industry for the last 12 years. Founder of SuperLight Industries, he's a security professional who has gained recognition on the web for websites such as GroupHug.us and BidItOnline.com. He resides in Atlanta with his beautiful wife, Lydia.*

***Gavin Mead (aka atlas)** is the product of a misspent youth hunched over the comforting glow of a green-and-black CRT. As monitor technology evolved, so did Gavin's interests in*

computer and network security, specifically in enterprise risk management frameworks and data privacy protection, leading him to the seedy underworld of security consulting where he met the the rest of the kaos.theory crew. Gavin currently works for KPMG's Security, Privacy, and Continuity practice out of Atlanta.

***Beth Milliken** pokes at computers for fun and profit, Beth has been sleeping lately in the wet spot where technology, ethics, and legal issues run together. She is very interested in educating people about protecting themselves on line - from not-so-nice people, as well as not-so-nice legislation. She works in a large building with lots of glass windows and foamy cube-walls. Beth has pieces of paper saying she is certifiable regarding certain bodies of knowledge, but swears she has no knowledge of where the bodies are.*

***Kevin Miller (aka digunix)** is one of the founding members of the DC404 group. Having recently moved back to Atlanta, he can be found near many a public access point with tools in hand. He needs a job BAD. Hook his ass up or he will make you his bitch. GO VEGAN!!*

Ripples in the Gene Pool - Creating Genetic: Mutations to Survive the Vulerability Window

Chris Eagle, Senior Lecturer of Computer Science

Reverse engineers often like to argue that a prime motivator for their activities is the desire to discover and patch vulnerabilities in closed-source binary software. Given the veritable plethora.. nay, Katrina-like flood of vulnerabilities being discovered on a near daily basis, one has to wonder where all these binary patches are hiding. Clearly this argument is a sham to make reverse engineers feel better about their DMCA violating activities. Now, just to be clear, there have been one or two third party binary patches released in the past year, but why haven't there been more? Is it truly a difficult task to develop such a patch or are our sights simply set too high? Is a true fix to the problem a requirement or is it sufficient to modify the vulnerable program just enough to make it immune to scripted attacks, the goal being to provide sufficient protection to survive until a vendor supplied patch can truly fix the problem. Dan Geer argued that a software monoculture is a dangerous thing leading to the rapid spread of malicious code in the event of a public vulnerability disclosure. The goal of this talk is to discuss simple yet effective measures to introduce sufficient genetic diversity into an inbred piece of software to allow it to survive in the wild until a vendor supplied update becomes available.

***Chris Eagle** is a DefCon Black Badge holder, and the Dean of Hacking for the Sk3wlofroot. When not at a CTF table, he is the Associate Chairman of the Computer Science Department at the Naval Postgraduate School (NPS) in Monterey, CA. A computer engineer/scientist for 20+ years, his research interests include computer network operations, computer forensics and reverse/anti-reverse engineering. He has been a speaker at conferences such as Black Hat, CodeCon, and Shmoocon and is a co-author of the book "Gray Hat Hacking".*

10 Ways To Not Get Caught Hacking On Your Mac

Charles Edge, aka Krypted, Partner, Three18

It's hard to prosecute someone if you can't prove what they did. In this session, we will quickly cover 10 easy ways to cover your tracks using Mac OS X. The features of Mac OS X at the GUI level were in a lot of ways designed to cater to the paranoid (eg. Steve Jobs). Underneath the hood, using some easily scriptable techniques you can cover your tracks in such a way that will make it easy to hide what you've done as well as your identity.

In this session, we will quickly cover some of the techniques that can be used to cover your tracks using case studies that illustrate ways that we have pieced together evidence as a starting point. Using a little bit of forensic evasion can go a long way to keep you free. This might also be interesting for forensic enthusiasts who can learn ways around these techniques.

***Charles Edge** began his consulting career working with Support Technologies, Andersen Consulting and Honda to name a few. In January of 2000 Charles arrived at Three18, a boutique consulting firm in Santa Monica, California. At Three18, Charles has worked with Network Architecture, Security and Design for a wide range of clients. As a partner at Three18 Charles manages a team of engineers, security professionals and programmers.*

His first book, "Mac Tiger Server Little Black Book" is available through Paraglyph Press. His second book, "Web Admin Scripting Little Black Book" is also available through Paraglyph Press. The latest title Charles is working on is Mac Security Essentials.

Mac OS X Security Tools

Charles Edge, aka Krypted, Partner, Three18

Apple claims not to care about the enterprise market, but there is no doubt that Apple networks are growing. The number of Apple systems in enterprise networks are growing as well. For security purposes it is becoming more and more important to manage these systems in the same way that we manage Windows clients.

In this session we will cover the tools that Apple and some 3rd party organizations have been quietly building for use in these environments. We will also cover the methods Apple has started using to facilitate running security updates on their workstations.

This is a good session for security professionals who have Mac systems on their networks. Tools we will cover:

- Mac OS X Server Managed Clients
- Nagios
- Radmind
- Apple Remote Desktop
- HenWen
- Tripwire
- Open Directory Password policies
- ipfw and dummynet
- Centrify DirectControl
- Dave
- AdmitMac

Securing MANET

Riley "Caezar" Eller, Director for Technology and Security, CoCo Communications

Mobile Ad-Hoc Networking (MANET) technology promises disaster-tolerant, interoperable, secure communications that work the way we users do. Features like automatic peer discovery and stable multi-transport TCP connections are so attractive that some may wonder if it isn't all too good to be true. After a brief but clear introduction to the more-or-less subtle differences between wireless routing technologies, we will delve directly into simulating attacks on Layers 2 and 3 and implementing appropriate defenses. Full graphical visualization of the processes and results makes this presentation accessible to anyone with at least basic understanding of computer networks.

As a professional software developer, Caezar began his career in embedded operating system development. After bringing that company to the Internet and integrating a TCP/IP stack, his passion for networking ignited. After a brief stint performing security audits, Mr. Eller returned to software development as the principal architect Greg Hoglund's ClickToSecure. He is only now resurfacing after spending three years bringing security and quality of service to high-speed mobile networks.

As the public face of the Ghetto Hackers, Caezar was central to DEFCON's Capture the Flag contest for the better part of a decade. During that time, he improved security contest scoring techniques, invented self-decoding ASCII-only stack exploits, produced fully automated web intrusion, and contributed to several other inventions including a pattern language for describing network attack processes.

DNS Abuse Infrastructure and Games

Gadi Evron

DNS operations today are no longer just a secure configuration and bandwidth, but rather a whole world of online abuse and criminal activities. In this presentation we will discuss how DNS has become this infrastructure for online crime and abuse. Spam, DDoS attacks, botnets and extremely reliable phishing servers all owe their existence to

DNS games. Further, we will discuss how DNS helps discover and combat malicious activities online and some of the Big Brother privacy risks this involves.

Gadi Evron *is a known leader in the world of Internet security operations, and especially in the realm of botnets and phishing. He was previously the Israeli Government Internet Security Operations Manager, as well as the Israeli Government CERT Manager. Today, he manages the SecuriTeam portal and works for Israeli-based Beyond Security.*

Analysing Complex Systems: The BlackBerry Case
FX, Phenoelit & SABRE Labs

When trying to analyze a complex system for its security properties, very little information is available in the beginning. If the complex system in question contains parts that the analyst cannot see or touch, proprietary hardware and software as well as large scale server software, the task doesn't get any easier. The talk will tell the story about how Phenoelit went about looking at RIM's BlackBerry messaging solution while focusing on the approaches tryed their expected and real effectiveness.

FX *is the leader of the Phenoelit group and loves to hack pretty much everything with a CPU and some communication, preferably networked. FX looks back at as little as eight years of (legal) hacking with only a few Cisco IOS and SAP remote exploits, tools for hacking HP printers and protocol attacks lining the road. Professionally, FX runs SABRE Security's consulting arm SABRE Labs, specializing in reverse engineering, source code audits and on-demand R&D of industry grade security architectures & solutions.*

MatriXay—When Web App & Database Security Pen-Test/Audit Is a Joy
Yuan Fan, Founder, DBAppSecurity Inc.
Xiao Rong

This topic will present a new web-app/DB pen-test tool. This tool supports both proxy (passive) mode as well as direct URL targeting. It is a mixed Web App SQL Injection systematic pen-test and WebApp/Database scanner/auditing-style tool and supports most popular databases used by web applications such as Oracle, SQL Server, Access and DB2. It has many unique features from web app backend Database automatic detection to the ability to browse database objects (without the need to ask for a passwords, of course), to the ability to locate/search for any sensitive content inside the DB and find more vulnerability points from source as well as privilege escalation.

Yuan Fan, *GCIH, GCIA, CISSP, is the founder of DBAppSecurity Inc with consulting service on enterprise security management especially on database and application security. His expertise spans from network layer to application/database layer Security. Before that he worked 5+ years for ArcSight for a variety of security device,s connectors, and many years in network management area.*

RE 2006: New Challenges Need Changing Tools
Halvar Flake, CEO of Sabre Security

Reverse Engineering has come a long way—what used to be practiced behind closed doors is now a mainstream occupation practiced throughout the security industry. Compilers and languages are changing, and the reverse engineer has to adapt: Nowadays, understanding C and the target platform assembly language is not sufficient any more. Too many reverse engineers shy away from analyzing C++ code and run into trouble dealing with heavily optimized executables. This talk will list common challenges that the reverse engineer faces in the process of disassembling nowadays, and suggest some solutions. Furthermore, a list of unsolved problems will be discussed.

Halvar Flake *is SABRE Labs' founder and Black Hat's resident reverse engineer. Originating in the fields of copy protection and digital rights management, he gravitated more and more towards network securityover time as he realized that constructive copy protection is more or less fighting windmills. After writing his first few exploits he was hooked and realized that reverse engineering experience is a very handy asset when dealing with COTS software. With extensive experience in reverse engineering, network security, penetration testing and exploit development he recently joined Black Hat as their main reverse engineer.*

Graphical Representations of Security Relationships: Awesome or Bullshit?

Foofus

We all want to be awesome hackers, but let's face it: inventing the sploitz can be hard work. What if there were a way to make interesting security discoveries using relatively simple tools, recycled concepts from research in other fields, and readily available data? For better or worse, this is the kind of question that we at foofus.net ask ourselves on a regular basis. And it's in that spirit that we present this fine talk.

We'll show some incremental advances in our penetration testing tools (once again, focused on identifying and taking advantage of trust relationships between Windows systems), and we'll appropriate concepts from graph theory. Our main goals are twofold. First, we want to find ways of mining new conclusions out of the same old data that's been staring us in the face all along. Second, we want to find ways of making the data we collect more interesting and useful. Basically, we're trying to look cool without having to work too hard.

Previously, we've provided tools for gathering this sort of information, and for representing it mathematically and visually. This year's talk focuses on using these techniques to draw worthwhile conclusions and offer helpful advice. As usual, our tools will be provided (such as they are), and a good time will be had by all.

Foofus *leads a team of security engineers at a technology consulting firm in the midwest, where he has worked for the past nine years. He has spoken at a variety of events and conferences including DefCon, ToorCon and LISA. His chief technical interests are software security, and the security relationships that emerge between systems in large networked environments. In his spare time Foofus enjoys playing guitar, cooking, and attending the opera and symphony.*

Ipv6 World Update: High Diplomacy & Monster Trucks

Kenneth Geers

Alexander Eisen

Governments around the world are investing serious time, effort, and money into the next gen Internet, based on IP version 6. With important mandatory and remarkably close deadlines looming for v6 deployment, much yet remains to be understood about its security and socio-economic implications as well as our readiness to fully embrace it. While Europe and Asia have been trailblazing IPv6 industry for years now, the U.S. Government has mandated that its organizations be IPv6-compliant by June 30, 2008, yet the vague definition of compliance has already confused many considering dual-stack, tunneled and/or native environments.

Imagine the bliss of IPv6 telematics, mobility, autoconfiguration, "mandatory IPSec" encrypted traffic and enough IPs to globally address everything with a battery or even a reference to a snippet of code for the world to access. Now imagine your firewalls and IDS sensors being blind to IPSec or even just cleartext 6to4 tunneled traffic. Debunking many myths, such as IPv6 "built-in security", prior to the transition is key as we watch the beloved IPv4 become legacy, say goodbye to NAT and the 6bone and welcome more DNSSEC, tunnel brokers and distributed PKI firewalls?!

This presentation will cover wide-ranging research the authors have conducted and the new paradigm shift necessary to approach IPv6 differently than IPv4, including interviews with some of world's top thinkers about the sleeping giant. Whether it is yet another gov-hyped failed theory like GOSSIB or it is here to stay, you will take away enormous insight into the work that you may be responsible for and dependent on over the next several years.

Alexander Eisen will present the tactical, down-in-the-weeds view of this elegant and extensible yet dangerous protocol. A threat analysis will follow, based on how the attack surface will inherently increase with the introduction of v6, many more IPs, more stacks, lack of smart fully v6-capable firewalls/IDSs and most importantly lack of training and understanding of this technology. Many are unaware of existing rogue v6 traffic on their networks and with Teredo's exploitation of NAT via UDP (enabled by default in XP SP1/2, Vista and Longhorn), your ::1 might already be owned... Some large enterprises can barely even inventory all their IP-enabled assets. Mr. Eisen will explain how attackers can use all this as ammunition to take advantage of the necessarily long-lasting, heterogeneous environment that will be required during the transition. Discussion of wardriving results and the efforts to build a v6 connection at home will also provide some intrigue.

Kenneth Geers will present the political and strategic view of IPv6, including why nation-states view the technology as vital to their national security plans for the future. Stops will be made at the White House, Beijing, Red Square, and Tokyo—all of whom are influencing the development of IPv6 standards in unique ways. He will cover the most current v6 research and deployment events from around the world, including translated summaries of official foreign language IPv6 documents that might otherwise remain inaccessible outside their home countries. DEFCON audience members should know that if some governments get their way on here-to-fore esoteric issues such as traceability due to privacy EUI-64 fields and IPSec certs, global v6 address allocation and portable IPs, they could well lose their last byte of anonymity on the Internet!

Last but not least, a live, on-stage demonstration will take place. The demo will show a discovery and port scan of the appliance via the Internet (found at this v6 IP -> 1337:sec:badd:a22:DEF:C012::14), followed by authentication, remote administration, and an SMS message sent to the speaker's mobile phone. Welcome to the v6-pack!!

Kenneth Geers *(CISSP, M.A. University of Washington) has worked for many years as a translator, programmer, Web developer, and analyst. The oddest job he has had was working on the John F. Kennedy Assassination Review Board. Mr. Geers is the author of "Cyber Jihad and the Globalization of Warfare", "Hacking in a Foreign Language: A Network Security Guide to Russia", and "Sex, Lies, and Cyberspace: Behind Saudi Arabia's National Firewall". His website, www.chiefofstation.com, is devoted to the intersection of politics, art, and the Internet.*

Alexander Eisen *(CISSP, M.S. University at Buffalo) has twice been awarded a government Information Assurance Scholarship to complete a multi-disciplinary Computer Science program spanning Cryptography, Cyber Law and Management. Having played in the fields of network red teaming, pen-testing, incident response, forensics and security product evaluation, his passions include exploring pioneering topics in security, researching with academia and being a bilingual grayhat-entrepreneur. Mr. Eisen attempts to give back to the community as an adjunct professor with University of Advanced Technology and an active member of IEEE Computer Society, Infragard, and AFCEA.*

Hardware Hacking

Joe Grand, President and Principal Electrical Engineer of Grand Idea Studio

Joe Grand *is an electrical engineer and prolific inventor with four pending patents and 19 commercially-available products. Involved in computers and electronics since the age of 7, Joe has had the fortune of being a former member of the legendary Boston-based hacker collective Lopht Heavy Industries, testifying before the United States Senate Governmental Affairs Committee under his nom de hack, Kingpin, and being praised as a "modern day Paul Revere" by the Senators for his research and warnings of computer security weaknesses. Recognized for his unconventional approaches to product development and licensing, Joe is also a well-known hardware hacker and industrial artist, the author of two books, contributor to four others, and is on the technical advisory board of MAKE Magazine.*

Fighting Organized Cyber Crime – War Stories and Trends

Supervisory Special Agent Thomas X. Grasso, Jr., Federal Bureau of Investigation

As one of the pioneers of partnerships for the FBI, Thomas X. Grasso, Jr. of the FBI's Cyber Division will outline how the FBI has taken this concept from rhetoric to reality over the past 5 years. This presentation will explore how the mantra "make it personal" has aided the FBI in forging exceptional alliances with key stake holders from industry, academia and ln a enforcement both domestically and abroad. This presentation will also outline how such collaborations have helped to proactively advance the fight against an increasingly international and organized, cyber crime threat.

Tom Grasso *began working with computers in 1993 as a network administrator. In 1998 Mr. Grasso received an appointment to the position of Special Agent with the Federal Bureau of Investigation (FBI). Mr. Grasso is now part of the FBI's Cyber Division and is assigned to the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh, a joint partnership between law enforcement, academia, and industry. Mr. Grasso is a 1991 graduate of the State University of New York at Buffalo, where he majored in Geological Sciences and minored in Music.*

First We Break Your Tag, Then We Break Your Systems Attacks to Rfid Systems

Lukas Grunwald

This talk provides an overview of new RFID Technologie used for Dual-Interfaces Cards (Credit cards, Ticketing and Passports), and RFID Tags with encryption and security features.

Problems and attacks to these security features are discussed and attacks to these features are presented. After dealing with the tags an overview to the rest of a RFID-implementation, middelware and backend database and the results of special attacks to this infrastructure is given.

At the end of this talk there is a practical demonstration of these discussed attacks.

Lukas Grunwald works for a German Security company, and has security experience over 20 years. As hobby he writes for the iX Magazine, and other security publications. He is also the head of the Hacking Lab where new technology is evaluated.

Phishing Tips and Techniques: Tackle, Rigging, and How & When to Phish

Peter Gutmann

This talk looks at the technical and psychological backgrounds behind why phishing works, and how this can be exploited to make phishing attacks more effective. To date, apart from the occasional use of psychology grads by 419 scammers, no-one has really looked at the wetware mechanisms that make phishing successful. Security technology doesn't help here, with poorly-designed user interfaces playing right into the phishers hands.

After covering the psychological nuts and bolts of how users think and make decisions, the talk goes into specific examples of user behaviour clashing with security user interface design, and how this could be exploited by attackers to bypass security speedbumps that might be triggered by phishing attacks. Depending on your point of view, this is either a somewhat hair-raising cookbook for more effective phishing techniques, or a warning about how these types of attacks work and what needs to be defended against.

***Peter Gutmann** is a researcher in the Department of Computer Science at the University of Auckland, New Zealand, working on the design and analysis of cryptographic security architectures. He helped write the popular PGP encryption package, has authored a number of papers and RFC's on security and encryption including the X.509 Style Guide for certificates, and is the author of "Cryptographic Security Architecture: Design and Verification" (published by Springer-Verlag) and the open source cryptlib security toolkit.*

Trust, But Verify: Auditing Proprietary DRE Systems

Robert J. Hansen, Researcher, ACCURATE

In 2006 the Help America Vote Act (HAVA) rid the country of lever voting machines and punchcard ballots, and gave the states enormous budgets for buying electronic voting machines. What's still unresolved is how these electronic voting machines are going to be audited. Trying to keep track of many different vendors, each of which has many different machines, is like getting lost in a funhouse hall of mirrors. Yet, there is good news. The National Science Foundation has established a research group for electronic voting, ACCURATE. In this presentation, an ACCURATE researcher will start talking about the thorny problem of making sure voting machines are playing fair. Existing technologies, both proprietary and open source, will be criticized; and new technologies will be presented.

***Robert J. Hansen** has a Bachelor of Arts in Computer Science, Cornell College, 1998. Master of Computer Science, the University of Iowa, 2006. Chief Security Geek for Yomu Inc., 2000. Cryptographic Engineer for PGP Security, 2000-2001. Student at the University of Iowa pursuing a Ph.D. in computer security, 2002-present.*

Your Name, Your Shoe Size, Your Identity? What do we Trust in this Web?

Seth Hardy

The web of trust, as used in PGP, is a well-known system for establishing trust between people, even if the people have not previously met. Why does it work so well in crypto? The answer is simple: it's the same system that we all use on a daily basis when dealing with friends, family, relationships, andjust about everyone else we have to

interact with. On the crypto side, however, there are a number of restrictions that limit the effectiveness of this trust network. While many "security professionals" say that they are mandatory, the system seems to work just as well without them— are they completely arbitrary? Here we'll look at a couple of these restrictions, focusing on the technical aspects of identity verification, and evaluate their effectiveness through a couple of real-world experiments.

Seth Hardy *stopped writing these self-promoting blurbs a long while ago. While he acknowledges there's far too much information about him on the internet already, he's been told that just saying this doesn't look too good standing by itself in a bio.So, here's some supporting facts: he's been involved in cryptography research, academically and professionally, for the last eight years. Some of these areas of research include elliptic curves, combinatorial cryptography, random number generation, and trust networks.*

Automatic Exploit Detection in Binaries
Matt Hargett
Luis Miras, Lead Vulnerability Researcher, Intrusion Inc.

Binary disassembling and manual analysis to find exploitable vulnerabilities is a cool topic. What's cooler? Saving yourself hours of time and brain rot by letting a program do the hard parts for you! In this talk, we will dissect a well-known exploitable vulnerability as well as an open source tool for automatically detecting that vulnerability. By the end of the talk, you will understand the basics of static code analysis, exploitable bugs in Windows, x86 assembly, and the structure of the open source project. Interested attendees can join a pair programming session after the talk to start work on enhancements.

Matt Hargett *last spoke at Defcon about using open source tools to test Firewalls and IDSes, and has spoken and written articles in a variety of venues and leading publications on the topics of security, testing, and programming techniques. After successfully creating and launching the commercial static analysis tool, BugScan, as the initial sole developer, he took time off and now works in a very different and unrelated field. He lives in Mountain View, California with his husband, Geoff, and their dog, Baxter.*

Luis Miras *is the lead vulnerability researcher at Intrusion Inc. He has done work for leading consulting firms. and Network Associates. He released the first public polymorphic shellcode at Defcon 8 and has also spoken at Toorcon 7 as well as the CCC Congress (17c3) in Berlin. In the past he has worked in digital design, and embedded programming.*

Remote Pair Programming and Test-driven Development Using Open Source
Matt Hargett
Luis Miras, Lead Vulnerability Researcher, Intrusion Inc.

Pair programming and test-driven development are proven best practices for producing high quality code quickly. But, because of geographical disparity, they can be difficult to apply to open source projects. This talk addresses how a flexible approach can be taken using open source software to enable this kind of collaboration. Attendees will learn the basics of the techniques, what tools to use (and not to use), and how it can improve their code no matter what language or platform they write it in.

WarRocketing – Network Stumbling 50 sq. miles in < 60 sec.
Rick Hill, Senior Scientist, Tenacity Solutions, Inc.

Network "stumbling" has taken many forms since Marcus Milner first released Netstumbler in May 2001. Historically, stumbling aficionados preferred data collection method has been Wardriving – almost everyone owns a car and it's easy to fire up your laptop and drive around. Of course, other methods exist...creative souls have utilized everything from bikes, to boats, to planes in pursuit of new networks. Groups in the U.S. and Australia have performed "WarFlying" using Cessnas and other, small aircraft.

Enter a newer (& faster) technique: "WarRocketing".

This talk is about 802.11b network discovery. It details the design, launch, and recovery of a rocket whose objective is to network stumble 50 square miles in less than a minute. Wardriving coverage is limited by obstructions such as trees, houses, and terrain. Our aerial platform, (the Rocket) does not have these limitations. Essentially, it provides Line-of-Sight to ALL targets in the antenna pattern!

The Presentation will include photographs of the rocket construction, (1/3 scale model Nike Smoke), a launch video, and screen capture & analysis of all computer activity during the flight: network stumbling, # of A/P's registered, and so on. No prerequisite—only an interest in Network Stumbling and Wireless Technology.

Rick Hill, *CISSP, CWSP works as an information systems security engineer for Tenacity Solutions, Inc., an IT consulting firm based in Reston, VA. Specializing in Wireless Security, his day job involves C&A of govt. networks, site surveys, and performing network security assessments. Rick's after work interests include working to become his neighborhood's Wireless Internet Service Provider (WISP), Netstumbling, and shooting High Power Rockets.*

Exploring the Changing Nature of DEFCON over the Past 14 Years
Dr. Thomas J. Holt, Assistant Professor, University of North Carolina at Charlotte

DEFCON began in 1993 as an "orgy of information exchange, viewpoints, speeches, education, enlightenment...and most of all sheer, unchecked PARTYING."(DEFCON 1 Announcement, 1993). Fourteen years later, the convention is one of the most established hacker conventions, and is defined as "the largest underground hacking convention in the world." However, significant social and technological changes have occurred during this period. The growth of the Internet, the increased need for computer security and the increasing significance of computer crime may have critically affected the shape and scope of the convention over time. This talk will critically examine the DEFCON convention over the past 14 years to understand the ways the con has changed, using previous convention materials, including programs, panels, and websites. The content, nature, and scope of the convention will be considered, including the number and types of presentations, as well as the presenters' credentials. This information will be assessed to consider what this says about the nature of the convention and the underground after 14 years. Audience participation is welcomed to inform this discussion and provide first hand insight into the past, present, and future of DEFCON.

Dr. Thomas J. Holt *is an Assistant Professor in the Department of Criminal Justice at the University of North Carolina at Charlotte specializing in computer crime and technology. His research interests include a variety of topics in computer and cybercrime, especially hackers and hacking. Over the past few years, Dr. Holt has examined the elements that compose hacker subculture, as well as hacker social organization through multiple data sources. His primary goal is to understand various social aspects of hacking and the computer underground from the hacker's perspective.*

Meme Hacking - Subverting The Ideosphere
Broward Horne, Software Consultant"Meme Hacking – Subverting The

IdeoSphere" is a followup and expansion of last year's "Meme Mining" presentation. It expands upon previous material and shifts from passive data mining to active meme manipulation. Concrete examples and patterns for meme manipulation are demonstrated, including an example of how I legally used active meme propagation to disrupt a former employer. The material ranges from specific tactical examples up to a strategic framework for Meme theory and the possible evolution of memes due to information technology changes.

Broward Horne *is a software consultant with a diverse background. He has done contract work for Unigard, Nike, JP Morgan, Verizon, Transcore and the US Department of Transportation, worked directly for several large corporations (Hewlett Packard, Avnet, Teradyne, Litton) and for two startup companies. His projects include network construction and administration, prototype wireless LANs, prototype pen-top software, CRM software, e-commerce, insurance and banking enterprise applications. Horne began data-mining & business intelligence in 1993 as a career guidance tool and have slowly expanding the scope, strategy and theory of my technique.*

Owning the linksys wrtp54g VOIP Router
Arias Hung

The wrtp54g/rtp300 is a linksys VOIP Proxy router with one primary distinguishing characteristic that separates it from all other VOIP Routers on the market today: It's based on linux.

This fact alone makes this router the key to learning the inner workings of VOIP and opens up a world of possibilities when it comes to its de-obfuscation. After all, 3rd party

firmware on its parent router, of which it is a descendant of the wrt54g, is big business as they've become near ubiquitous in every consumer household. With VOIP poised as the current cat-out-the-box technology prepped to take down established telecoms, VOIP security takes front and center as a paramount imperative.

The problem to this point has been this router being tied specifically to one vendor, who happens to also be the largest VOIP only vendor to date whose interest is that your hard ware can be only used for their service.

Discover how vendor provisioning works on these routers, in order to reclaim control of your hardware. Learn specifics as to the ar7 dual processor architecture that the hardware utilizes, and how to unlock its numerous built-in capabilities that have been crippled prior to release by the vendor. Watch a demonstration of how easy VOIP and its companion protocol MGCP can be manipulated for illegal purposes such as call spoofing, number hijacking, and untraceable call routing. And find out how companies that provide VOIP are complying with the FCC mandate that requires them the ability to snoop at will without a court mandate, by saving all of your voice calls as a .wav file that can be listened to at their leisure.

Arias Hung *is a security professional with a particular passion for embedded distributions. Arias began his career in unix administration, specializing in SGI/Irix while employed at the Lawrence Berkeley National Laboratory (lbl.gov) before expanding independently as a Unix consultant in silicon valley and gaining a degree in computer forensics and security. Arias is currently working as a security consultant in the Seattle area.*

How to Create an Anonymous Identity
Johan Hybinette

An Anonymous identity is difficult but not impossible to obtain. With help of international laws and loopholes a new identity can be created.

This talk will demonstrate how this can be done with never before published methods.

There are many reasons why a person might choose to obscure their identity and become anonymous. Several of these reasons are legal and legitimate - someone, for example, who feels threatened by someone else might attempt to hide from the threat behind various means of anonymity. There are also many illegal reasons to hide behind anonymity. Criminals typically try to keep themselves anonymous either to conceal the fact that a crime has been committed, or to avoid capture.

Johan Hybinette *is CSO and founder of Cebic Technologies, inc. specializing in international security auditing, policy and monitoring. Johan has over 20 years of security experience and has been speaking on numerous international events. His expertise includes compliance, pen testing, SIM integration (Security Incident Management), auditing, and identity management. Some of the certifications held are CISM, CISSP, ISSAP, IAM, ISSMP, IEM.*

Black Ops 2006
Dan Kaminsky

The known topics for this year include:

1. The Worldwide SSL Analysis—There's a major flaw in the way many, many SSL devices operate. I'll discuss how widespread this flaw is, as well as announce results from this worldwide SSL scan.
2. Syntax Highlighting...on Hexdumps. Reverse Engineering efforts often require looking at hex dumps—without much context for whats being looked at. I will discuss a "bridge" position between AI and manual operation in which compression code is used to automatically visualize patterns in analyzed data.
3. Everything else

Dan Kaminsky, *Dox Para Research. Formerly of Cisco and Avaya.*

Oracle Rootkits 2.0
Alexander Kornbrust, Founder & CEO, Red-Database-Security GmbH

In 2006 thousands of people will create applications based on the free Oracle 10g Express Edition. Even if this version of Oracle (based on Oracle 10g Rel. 2) is the most secure database from Oracle out of the box so far, there is still room for improvements.

This presentation shows different possibilities to attack Oracle 10g Express Edition (and Oracle 10g Rel. 1 and Rel. 2).

With Oracle 10g Oracle introduced some new security features (e.g. listener protection) which eliminates old attack vectors. But by introducing new features they implemented new bugs and new possibilities like SQL injection, built-in HTTPS-server, etc

Alexander Kornbrust *is the founder and CEO of Red-Database-Security GmbH, a company specialized in Oracle security. Red-Database-Security is one of the leading companies in Oracle security. He is responsible for Oracle security audits and Oracle anti-hacker trainings.*

Alexander Kornbrust has worked with Oracle products as an Oracle DBA and Oracle developer since 1992.During the last six years, Alexander has found over 220 security bugs in different Oracle products.

Hacking UNIX with FreeBSD Jail(8), Secure Virtual Servers

Isaac Levy (.ike)

FreeBSD Jails are a time-tested, secure UNIX virtual machine with endless uses.

Early unix mainframe computing brought elegant process and resource sharing systems, which helped get more application use out of expensive hardware. These concerns have been largely been pushed aside in computing with the rise of desktop PCs, and large farms of ever-shrinking pizza boxes in the data center. Today, as more punch gets packed into 1u than ever, server resources can be further consolidated and abstracted to securely separate complex and sophisticated services in the same hardware server, by running secure virtual UNIX machines.

Who wants jails?

System Administrators who need to securely separate small yet important services.

Software Developers who always need more dev machines to hack amok.

Root-Kit Testing and Debugging.

Educators who could use virtual machines to provide clean unix server systems for student use.

Anyone who wants *secure* virtual machines.

Why would you want jail(8)?

The design of Jail(8) and jail(2) are small and secure, and because jails use native system utilities, they are simple for any unix hacker to work with- very shallow learning curve. They're great for userland-level hacking and development, honeypots, or highly available services for regularly attacked systems.

What I'd like to talk about:

- How Jails Work, the technical nitty-gritty
- How to setup jails, the practical how-to, cooking show style...
- When NOT to use jails
- jail(8) security vulnerabilities/considerations, attacking and breaking out of jail(8)
- o mitigating the risks of attacks and jail(8)breaks
- Jails vs. Linux UML, XEN, VMware- fundamental technical differences

Isaac Levy, (.ike) *is an Open Source web-application developer based in New York City. He runs Diversaform Inc. as a business platform to make his code feed itself, (and ike). Diversaform specializes in BSD based solutions, web applications, and specialty network applications. Ike works as an consultant/developer mostly with small and medium sized business, but periodically works within large corporations and organizations.*

Advanced Windows Based Firewall Subversion

Linoxx

This presentation will focus on disabling many of the windows based network security solutions that are most widely used. New payloads will be presented that demonstrate how host based firewalls at this time are not adequate defense to safeguard one's network resources. The speech is highly technical and requires knowledge of reverse engineering and process injection.

Linoxx *has been a code and security enthusiast for a number of years along with speaking at interzone 5. He also helps run the local DC group in Atlanta, DC404.*

Death By 1000 cuts

Johnny Long / johnny

In this day and age, forensics evidence lurks everywhere. The task presented to modern forensics investigators is a daunting one. During this talk, you'll slip into the shoes of an uber-agent hot on the trail of the illustrious Knuth from the Stealing the Network series. Haven't read the latest installation? You should. How would YOU catch a guy that MELTED his hard drive platters and sanded down all his CDs? Where's the evidence? That's the question of the hour. Answer it correctly and you could win any number of cool prizes.

Now that the talk description you can show you boss is out of the way, what's this really about? Think of it as the hacker's version of "Where's Waldo." You'll laugh. You'll learn. You'll cry when you realize the answer was staring you right in the face. You'll scream when you're caught in the mosh pit of the full-on frenzy of the bonus prize rounds. Forget Waldo. This is HALO 2 meets hacking. Get your game on. Got no coordination, no reflexes, no skillz, and no eye for detail? Come anyway.

Come have some fun, and learn how the feds put the smack down on even the most paranoid among us.

Johnny Long *is a "clean-living" family guy who just so happens to like hacking stuff. A college dropout, Johnny overcompensates by writing books, speaking at conferences and hanging around with really smart people. Johnny is currently working on the final third of the coveted "Hacker Pirate Ninja" title, which has thus far evaded even the most erudite of academics. Johnny can be reached through his website at http://johnny.ihackstuff.com*

Secrets of the Hollywood Hacker!

Johnny Long / johnny

Hacking stuff is for the birds. I'm taking a new path in life. I've decided to become a technical consultant for Hollywood. (No, not really, but work with me here). In my new role, I've decided it's time to take up the torch for all my fellow consultants who have been abused by you people through the years. We're all just sick and tired of your snide little comments about hackers in the movies.

So go ahead. Make fun of Hollywood. Poke fun at A-list actors who "slide in [a] Trojan horse riding a worm" or B-movie bandits that use "mega modems with compression". Snort your snooty little snicker at smarties who smash 128-bit DES encryption in a skimpy 60 seconds. Who do you think you are, anyway? You've probably never even USED 128-bit DES. Think you're all über because you can sling a bit of code? Let's see you sling a multi-headed worm that sniffs out latent digital footprints throughout an encrypted network. Not leet enough? That's OK. I'll show you how it's done.

Think you've found a movie line that's just slam-dunk stupid? A movie line that proves Hollywood is just clueless about technology? Think again. You just misunderstood. I'll use video clips and ultra-magnified freeze-framed screen stills to prove to you that Hollywood is clue++. Failing that, I'll at least distract you with seriously classified hardware and oday exploits that were leaked through Hollywood films. Then again, you just might be safer if you keep on thinking they're only cheesy movie props.

Old Skewl Hacking: Magstripe Madness

Major Malfunction

It's been a year since Major Mal gave his talk on hotel IR systems, and things haven't got any better...In fact, they've got worse. No, wait a minute...that's not right...They've *stayed* worse!! Having plumbed the depths of the IR in his room, and finding himself with little else to do, Major turned his attention to another piece of technology easily to hand: his magstripe room key...Now these have been around since Mary checked into her stable, and every hotel on the planet is using them, so they *must* be secure, right? Right??? OMFG, wrong! So wrong it'll make your head spin... In this talk Major Malfunction will expose not only how easy it is to bypass security mechanisms built into various magstripe technologies such as hotel doorkeys, train tickets, credit cards etc., but will also take a sideways look at how they might be leveraged to provide attack vectors on other in-house systems, such as passenger ticketing systems, bank clearing houses, hotel billing...OK, OK, enough already! We can fix this! All we need is some new technology, like, errr...RFID! That's it! That'll do the trick! Right? Right????

Major Malfunction *lives in a fantasy world. He believes he works by day in the security industry, advises corporate, government, police and military, has a base in a secret underground nuclear bunker, and a network of colaborators all over the world involved in dark mysterious missions. He legally indulges his love of firearms in a country that prohibits them, swaps souvenirs with TLAs from all over the world, and generally swans about the UK like he owns the place...If you look closely, the man is obviously James Bond... No, not that closely...Back a bit and squint so you can't see his paunch...That's it! There, you see? What's that bulge under his armpit? James Bond, definitely.*

Visual Log Analysis—The Beauty of Graphs

Raffael Marty, GCIA, CISSP, Manager Strategic Application Solutions, ArcSight

Event and Log Analysis is becoming one of the main tools for security analysts to investigate and comprehend the state of their networks, hosts, and applications. Recent developments, such as regulatory compliance requirements and an increased focus on insider threat has increased the demand for analytical tools to help in the process. Event correlation is one of the tools that helps addressing the challenges. However, the vast amount of events still leaves the analysts with enourmeous amounts of data to manually analyze, creating space for new tools to fill the gap.

Visualization of data has proven to be the approach generating the best return on investment. This talk takes a step-by step approach to analyzing a log file, showing how AfterGlow (afterglow.sourceforge.net) can be used to analyze and understand a log file. The analysis will show how visualization can be used to detect portscans, policy violations, and misconfigurations. The talk will focus on using link graphs and treemaps to analyze the data sets.

The goal of the talk is to leave the audience with the knowledge and tools to do visual log analysis on their own data. The main tool used for the talk is AfterGlow (afterglow.sourceforge.net), which in his current version supports a diverse set of operations to ease the analysis of log data.

Raffael Marty, *GCIA, CISSP is the manager of ArcSight's Strategic Application Solution Team. Raffael initiated ArcSight's Content Team, which holds responsibility over all the product's content, ranging from correlation rules, dashboards and visualizations to vulnerability mappings and categorization of security events. Before joining ArcSight, Raffael used to work as an IT security consultant for PriceWaterhouse Coopers and previously was a member of the Global Security Analysis Lab at IBM Research.*

Zulu a Command Line Wireless Frame Generator

Damon McCoy, University of Colorado at Boulder

Anmol Sheth

Zulu is a light weight 802.11 wireless frame generation tool to enable fast and easy debugging and probing of 802.11 networks. It has an intuitive command line interface and operates with the unmodified madwifi-ng and partially with prism based Linux network drivers. Individual fields in frames can be set or unset, generating frames that possibly violate the IEEE 802.11 protocol. It can generate all control, data, and management frame types and subtypes. The user-friendly command line options enable novice users to quickly generate custom frames with a combination of values placed in different frame fields. Zulu is freely available under the GNU license.

Damon McCoy *has worked in a variety of industry and government positions. Currently he is a Doctoral Candidate in the Department of Computer Science at the University of Colorado at Boulder. He has also worked at Sandia National Laboratories in the Center for Cyber Defenders. Prior to this he worked for IBM in the Emergency Response Services group as a network security consultant. Before this he worked for both AT&T Research and Lucent Bell Laboratories.*

Anmol Sheth *is a Doctoral Candidate in Computer Science at the University of Colorado at Boulder. He received his B.S. in Computer Science from the University of Pune, India in 2001. His research interests include MAC layer protocol design, fault tolerant distributed wireless systems and energy-efficient wireless communication.*

A New Bioinformatics-Inspired and Binary Analysis: Coding Style/Motif Identification

Scott Miller

Security analysis is severely complicated by the size and abundance of executable code. Existing concepts and code can be combined, obfuscated, packed, and hidden toward the ends of evading detection and frustrating analysis. Is that patch fixing the problem it claims to fix? Have you seen that malicious code before? Have you seen these particular motifs/style before?

All very interesting questions, some of which can be addressed using existing tools/techniques. This talk looks at a new tool, inspired by a scored string match used for genetic analysis: the Basic Local Alignment Search Tool (BLAST). Can this tool identify motifs common to UPX? Can this tool identify code generated by different versions of GCC? Does this tool provide similar Malware classifications to other tools?

The talk will include an overview of the technique, demonstration of the use of the new tool set (binBLAST), and its performance.

***Scott Miller** has recently graduated from the New Mexico Institute of Mining and Technology, the technique of this presentation developed in his Master's Thesis "A Bioinformatics Approach to the Security Analysis of Binary Executables". While pursuing his master's degree, he also considered a number of topics including human infection/immunity, natural language steganography, self-sustaining high-availability intrusion prevention systems, and secure compiler construction.*

Bridging the Gap Between Static and Dynamic Reversing

Luis Miras, Vulnerability Researcher, Intrusion Inc.

Reverse engineering continues to evolve, or rather REvolve. The reverse engineering toolset primarily consists of disconnected disassemblers and debuggers. Without symbol information or data acquired from disassembly, the use of a debugger can be blind and tedious.

Reverse engineering has fueled the need to enable these tools to work together. When disassemblers and debuggers are used in conjunction, the resulting union is greater than sum of the disparate parts.

To bridge the gap between disassemblers and debuggers, I will be releasing two IDA Pro plugins.

- pdbgen-Generates custom pdb files from the IDA Pro database. The pdb file can then be loaded into a debugger, transferring symbolic information.
- Redress-Reinserts debug information from the IDA Pro database into stripped ELF executables. The inserted debug information will be available in GDB.

During this talk, I will review the other tools and plugins that perform similar bridging functions. I will then present a live demonstration of pdbgen and REdress, streamlining the reversing process.

¡Viva la REvolución!

Rebuilding HARD DRIVES for Data Recovery; Anatomy of a Hard Drive

Scott Moulton, Forensic Strategy Services, LLC. / System Specialist

Every hard drive will die a quick and sudden death sooner rather than later. What happens after that death can be very important to your data and become the deciding factor in its survival. We will display the inner workings of a hard drive in a beautiful animation and discuss the successes and failures in rebuilding a hard drive. We will teach you what to look for and how to accomplish this task on your own. We will delve into the platters and heads to show you when there is a good probability of success. Have you ever wondered how data recovery houses can rebuild your drive and put your data back together? The animated presentations will make it clear how rebuilding a hard drive can save your data and your money.

***Scott Moulton** was the first person arrested for Port Scanning in January of 2000. During the defence, Scott found he had to train his lawyers on the technical aspects of computers in order to defend himself. This began his forensic computer career with a speciality in rebuilding hard drives for investigation purposes.*

Advanced Attacks Against PocketPC Phones

Collin Mulliner

Smart phones are the new favorite target of many attackers. Also most current attacks are harmless, since these mostly rely on user mistake or lack of better knowledge. Current attacks are mostly based on logic errors rather then code inject and often are only found by accident. The talk will show some real attacks against smart phones and the kind of vulnerability analysis which lead to their discovery.

Collin Mulliner *is a computer science student/researcher and a member of the trifinite.group. Collin's main interest are mobile devices, their security and pretty much everything that is somehow related. Collin started poking PalmOS-based PDAs in 1997, and by now has laid his hands on pretty much every existing type of portable device. In recent years Collin was mainly messing around with Bluetooth and created the first Bluetooth port-scanner. Lately Collin's main focus shifted towards PocketPC-based smart phones.*

Covert Channels using IPv6/ICMPv6

R.P. Murphy

Government organizations are required by the Office of Management and Budget to migrate their networks over to IPv6 by 2008. There is a belief that this opens inherit risk to the organization due to undiscovered flaws and security holes that may be opened up. One such breach is the use of covert channels to push data in or out of a network in the guise of standard traffic. Covert channels are not new, and have been exploited in the past through IPv4 communications. This presentation and PoC tool demonstration will show how IPv6 networks communicate, and how the tool can be used to pass text or files through IPv6 and ICMPv6 packet manipulation.

R.P. Murphy *is currently pursuing a Masters Degree in Information Systems Technology and is working on IPv6/ICMPv6 Covert Channels as a thesis topic. Areas of interest include computer forensics, protocol analysis and tool development. Tools developed include MACSpoof, a tool to store and change MAC addresses in Windows, VoodooKey, a tool to recover software keys in Windows, and the PoC tool voodooN3t, a tool that sends text or files through the use of IPv6 / ICMPv6 packet manipulation.*

US-VISIT: Raping Personal Privacy Since 2004

Chris Paget, Director of Research and Development, IOActive Inc.

In 2004, the Department of Homeland Security began the deployment of US-VISIT—a system for tracking visitors to the United States. Since that time, the capabilities of US-VISIT have increased dramatically; US-VISIT now incorporates a number of controversial technologies which violate the privacy, anonymity, and overall security of visitors to the USA in significant ways.

In this talk, the technology and capabilities of US-VISIT will be explained in detail; weaknesses in the system will be explored, and the consequences of such a system will be considered. If you are a foreign national visiting the USA, a US citizen who is concerned about what DHS has in store for you, or just curious about what US-VISIT does and how it works, this is the talk for you.

Chris Paget *is the Director of Research and Development for IOActive Inc, based in Seattle. Recently, Chris has been working on the "biggest independent security audit in history"—the Final Security Review of Windows Vista. Chris is an expert on Windows architecture and security, a privacy advocate, a British expatriate, a helicopter pilot, and a Code Red junkie.*

"What has the NSA done for me lately?"

Timothy M O'Neill, Instructor, Div of Extended Studies, Boise State University

In 2002 the President issued an Executive Order authorizing the National Security Agency (NSA) to wiretap phone and email communications involving United States persons within the U.S., without obtaining a warrant or court order pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), which prohibits such unauthorized electronic surveillance. Investigate the technology timeline regarding this Contentious activity. The surveillance threat to liberty consists of multiple and overlapping collection efforts, targeted against all sources of information available by various agencies and is supported through several pieces of legislation. For this reason, the balance between technological capability and privacy will continue to remain a major concern in the future.

Tim O'Neill instructs various engaging INFOSEC and OPSEC courses as an adjunct professor with the Division of Extended Studies at Boise State University. Working extensively with the National Security Agency's Information Assurance Directorate, (NSA IAD) he was successful in designing and implementing the first NSA accredited curriculum for the Information Assurance Courseware Evaluation Program at Boise State University in accordance with the Committee on National Security Systems (CNSS) National Standards 4011 & 4013. As an associate of the FBI's Infragard Salt Lake City Utah chapter, he works to provide assistance, expertise and resources relating to Information Security vulnerabilities, policy development and computer security best practices. Additionally, Tim O'Neill is part of a collaborative effort with the Better Business Bureau to form a regional, small business training group, fostering trust and partnerships throughout business and industry, while providing risk mitigation, education, training and research modalities.

802.1x Networking

tommEE pickles, Security, Administrator, Moloch Industries

tommEE pickles (http://tommEE.net) presents an explanation of 802.1x networking. Exploring what 802.1x is and why we would use it. He explains how 802.1x might be used in a corporate environment, wireless or wired. Giving an explanation on how you can start 802.1x network and get your users on it. Hardware and Software resources will be discussed and recommendations for free ways of accomplishing it will be presented. He will talk about the current problems and how to provide possible fixes for problems.

***tommEE pickles** has been born, raised, and possibly living in New York City. He co-founded Moloch Indiustries in 1999. He his known for the 4 Defcon Cannonball Runs and his passion for Streaming Media and TiVo hacking. tommEE has worked for large streaming media providers while giving them solutions for streaming media security. He has also developed wireless networks for several large companies.*

Trusted Computing: Could it be... SATAN?

Bruce Potter, The Shmoo Group

Trusted computing is not inherently evil. It sounds scary, but it's true. While the public perception of trusted computing is that content providers will use trusted computing to enforce their digital rights and take away our civil liberties (whew! a mouthful), the reality is that there is a lot of good to be done by trusted computing.

For more than thirty years, computer scientists have been trying to find ways to make trusted computing a reality. Unfortunately the technology simply wasn't there, and info sec folk and hackers alike have spent their time chasing an impossible dream. Now we finally have the ability to have trusted hardware in general purpose devices and we need to figure out what to do with it. Everything we know about security changes with trusted computing...firewalls, SSL transactions, and even SMS have very different concerns with trusted computing than they do now. This talk will attempt to dispel some of the myths of trusted computing, discuss the current state of trusted hardware, and examine how software will change due to the TPM. Heck, we'll even have some tools for you to play with on your TPM-enabled hardware.

***Bruce Potter** is the founder of the Shmoo Group of security professionals, a group dedicated to working with the community on security, privacy, and crypto issues. His areas of expertise include wireless security, software assurance, pirate songs, and restoring hopeless vehicles. Mr. Potter has coauthored several books including "802.11 Security" and "Mastering FreeBSD and OpenBSD Security" published by O'Reilly and "Mac OS X Security" by New Riders. Mr. Potter was trained in computer science at the University of Alaska, Fairbanks. Bruce Potter is a Senior Associate with Booz Allen Hamilton.*

Service Cloaking and Anonymous Access; Combining Tor with Single Packet Authorization (SPA)

Michael Rash, CTO, Solirix, Inc.

Single Packet Authentication is becoming an increasingly important method for protecting arbitrary network services through the use of a kernel level filtering mechanism such as Netfilter in the Linux kernel. By sending SPA packets over the Tor

network, SPA packets can be endowed with an additional layer of privacy and anonymity. It becomes cryptographically difficult to deduce the communication of the SPA packet from any particular source address; even from the perspective of an attacker that is in the enviable position to montior all packets going to and leaving from the SPA client system. The end result it that the exploitation of even o-day vulnerabilities in a service that is protected with SPA/Tor is much more difficult. This talk will focus on applied aspects of Single Packet Authentication, and will include a lengthy demonstration at the beginning of the talk. A new version of the Single Packet Authentication software "fwknop" will also be released contains new features such as GPG-hardened last-hop IP resolution, a web interface to monitor SPA usage in an Enterprise environment, remote Netfilter policy management, and more.

Michael Rash *is the CTO of Solirix, Inc. where he leads the Solsen product development effort. Previous to Solirix, Michael was a developer on the Dragon intrusion detection and prevention system, and also wrote a custom host-based intrusion detection system which was used to monitor the security of over one thousand systems from Linux to Cisco IOS at a major ASP. Michael frequently contributes to open source projects such as Netfilter and Bastille-Linux. He is also the lead author of the book "Intrusion Prevention and Active Response; Deploying Network and Host IPS", and a co-author of "Snort-2.1 Intrusion Detection", both published by Syngress Press. Michael is the creator of two open source tools "psad" and "fwsnort" that are designed to blur the boundaries between Netfilter firewalls and the Snort IDS.*

New Wireless Fun From the Church Of WiFi
RenderMan, Sacramental Wine taste tester for the Church Of WiFi
Thorn, The Baby-eating Bishop of Bath and Wells
H1kari, CPU pimpmaster

The Church of Wifi (reformed) has been busy coming up with new and wonderful wireless shenanigans. At Shmoocon we sped up WPA cracking 3 fold, at Layerone we made it even faster, now we take it even further, to places and sizes not dared before: WPA2!

When we are'nt breaking WPA or cavorting with Evil Bastards, we are thinking about the future. With so many networking devices running embedded OSS software, they are almost whole PC's unto themselves. Well, what happens when hardware goes viral? The Church raises the question, "How do you trust your hardware?"

So bring your open minds and external hard drives, Church shouldn't ever be this fun.

Frank ("Thorn") Thornton *runs his own technology-consulting firm, Blackthorn Systems, which specializes in wireless networks and security. An interest in Amateur Radio has also helped him bridge the gap between computers and wireless networks. Thorn's experience with computers goes back to the 1970's when he started programming mainframes.*

In addition to his computer and wireless interests, Thorn was a Law Enforcement Officer for many years. As a detective and forensics expert he has investigated approximately one hundred homicides and thousands of other crime scenes. Combining both professional interests, he was a member of the workgroup that established ANSI Standard ANSI/NIST-CSL 1-1993 "Data Format for the Interchange of Fingerprint Information." Thorn is a co-author of "WarDriving: Drive, Detect, Defend", "Game Console Hacking", "RFID Security" and contributor to "IT Ethics" all by Syngress Publishing.

RenderMan *has been a fixture in the wardriving community for many years. He never seems to be out of crazy projects and ideas, never very far from wardriving news, often causing it himself. He also co-authored "RFID Security" for Syngress publishing. He spends his time working on things like the 'stumbler ethic', Worldwide wardrive, 'the warpack' and the Church of Wifi. When not working to make wardriving an acceptable hobby, he can usually be found taking something apart, creating an army of cybernetic fluffins, trying to win the Defcon wardriving contest, or more likely, at the hotel bar.*

David "H1kari" Hulton *has been in the security field for the past 7 years and currently specializes in FPGA Logic Design, 802.11b Wireless Security, Smart Card, and GSM development specifically to exploit its various inherent strengths and weaknesses.*

David Hulton is one of the founding members of Pico Computing, Inc., a manufacturer of compact embedded FPGA computers and dedicated to developing revolutionary open source applications for FPGA systems. He is also one of the founding members of Dachboden Research Labs, a non-profit security research think-tank, is currently the

Chairman of the ToorCon Information Security Conference and has helped start many of the security and unix oriented meetings in San Diego, CA.

A Hacker's Guide to RFID Spoofing and Jamming

Melanie Rieback, RFID Security/PrivacyResearcher, Vrije Universiteit Amsterdam

Radio Frequency Identification (RFID) tags are remotely-powered data carriers that augment physical objects with wireless computing abilities. This allows us to create smart homes and offices, optimize our supply chains, and keep a watchful eye on our pets, livestock, and kids. But unfortunately, RFID security and privacy issues have been addressed as an afterthought; it is regretfully easy to interfere with RFID systems, as many rely upon the integrity of RFID tag data for their correct functioning. To illustrate these problems, we have built a handheld device that performs RFID tag spoofing and selective RFID tag jamming (a bit like an "RFID firewall"). Compatible with the ISO 15693/14443 13.56 MHz RFID standards, our device is battery-powered and fits into a shirt pocket. This presentation will explain the "nuts and bolts" of RFID tag spoofing and jamming attacks, and will conclude with a live practical demonstration of these attacks.

***Melanie Rieback** is a Ph.D. student in Computer Systems at the Vrije Universiteit in Amsterdam, where she is supervised by Prof. Andrew Tanenbaum. Melanie's research concerns the security and privacy of Radio Frequency Identification (RFID) technology, and she leads multidisciplinary research teams on RFID privacy management (RFID Guardian) and RFID security (RFID Malware) projects. Melanie's recent work on RFID Malware has attracted worldwide attention, appearing in the New York Times, Washington Post, Reuters, UPI, de Volkskrant, Computable, Computerworld, Computer Weekly, CNN, BBC, Fox News, MSNBC, and many other print, broadcast, and online news outlets. Melanie has also served as an invited expert for RFID discussions involving both the American and Dutch governments. In a past life, Melanie also worked on the Human Genome Project at the MIT Center for Genome Research / Whitehead Institute.*

IBM Networking Attacks-Or The Easiest Way To Own A Mainframe Without Getting The Removals Men In

Martyn Ruks, Security Consultant, mwr Infosecurity

Why would you want to attack IBM Networking? Isn't it old, unused and unimportant in today's modern business environments?

The answer is why not attack it, after all it is still deployed in lots of high value environments. IBM Networking usually means Mainframes and therefore the potential to get to some cool financial or intelligence data.

But what was that I heard you say? You can only route IP across the Internet! Maybe so, but if you have a poorly designed network I just might be able to get to your mainframe. Maybe even compromise it!

So if you are a penetration tester, Security Manager or Network Architect you will gain insight into a number of areas of IBM Networking security. You will also learn about the tool which will be released to accompany the presentation.

This presentation will introduce the basic concepts behind a number of IBM networking protocols and how they are currently used by companies and will cover a number of areas including an overview of Systems Network Architecture (SNA) and Data Link Switching (DLSw). The manners through which these protocols can be abused to gain unauthorised access to systems will also be discussed. This presentation is not a criticism of IBM or their technologies but intends to lift the lid on an area of IT security that is not widely understood.

The presentation will cover issues relating to software bugs, device configuration and architecture design. A number of recommendations are also made to ensure that vulnerable environments can be adequately secured against attack.

***Martyn Ruks** is an information security professional working for mwr Infosecurity in the UK. Martyn has worked in the industry for 5 years and has principally been involved in security consultancy and penetration testing. This testing has covered a wide range of technologies and has been performed for Blue Chip companies. Very little of Martyn's previous security research has been published, however, this presentation is intended to form the first part of a detailed investigation into various IBM technologies.*

Safecracking Without a Trace

Eric Schmiedl

Despite many appearances in film and television, fairly little is widely known about how safes can be opened without the proper combination or key. This talk will attempt to address some of the questions commonly asked about the craft, such as— is it really possible to have a safe open in a minute or two using just a stethoscope and some clever finger-work? (Yes, but it will take a bit more time than a few minutes.) Are the gadgets used by secret agents in the movies ever based on reality? (Some of them.) The talk will cover several different ways that safes are opened without damage, as well as the design of one lock that is considered completely secure.

Eric Schmiedl *is studying mechanical engineering at the Massachusetts Institute of Technology. Since learning to pick locks in elementary school, he's taught lockpicking workshops at What the Hack 2005, opened safes for the MIT pistol team, and done contract work for M. Tobias, JD of Locks, Safes, and Security fame.*

Cyber-crime Foiled Once Again? Help prove the innocence or guilt of Jack Grove

Amber Schroader, CEO, Paraben

Tyler Cohen, Digital Forensics Instructor Department of Defense Cyber Crime Center

Jack Grove tries to stop his racing heart as he slips into a dark dingy alley. His paranoia is getting the best of him as he looks behind him. No one is following him, but he senses they are coming. He is afraid. The hack hadn't gone down as planned. Damn it, he was supposed to have taken everything into account, he got sloppy. He knew his only saving grace was no one would be able to recover his laptop. Not after what he did to it.

Jack pulls out his cell phone to make what will soon be his last phone call.

He looks around anxiously to make sure that he is alone before making the most important call of his life. He notices a man digging through a trash can. He decides not to risk the man overhearing him and chooses to send a text message instead. With his palms starting to sweat he texts:

"net hax. Hidn. Dngr. Plan?"

Just as the send button is pushed the alley is swarming with agents. Jack is thrown up against a wall. Agents begin to frisk him and take the remains of his hack from him. His cell phone, PDA, and iPod are all that is left of his digital task.

He watches and wonders will they find anything to tie him to what has just happened as he is taken away into custody.

Back at the crime lab, the agency's uber geek lab babes Amber and Tyler are under the gun to get this case solved. Someone on top thinks it is personal and wants Jack Grove. The two ladies are used to the pressure, but know they are tops in the crime lab when it comes to the bizarre bits and bytes of devices. They start their examination on the three items from the scene the cell phone, PDA and an iPod.

Can these two super sleuths use digital forensics on the few devices recovered to figure out what Jack Grove was up to, who his accomplices were, and find the evidence needed to prosecute?

By using this scenario, Amber and Tyler will bring the audience into the crime lab with them. Taking the devices from seizure to analysis showing where Jack Grove has left his digital fingerprints. Once the fingerprints are gathered the audience will work with these two examiners to piece together the case and solve the crime and prove Jack's innocence or guilt.

The audience will gain an overall understanding of digital forensic handling and procedure. Details to what is gained on some of the unique digital storage devices will be demonstrated.

Amber Schroader *has been involved in the field of computer forensics for the past seventeen years. During this time, she has developed and taught numerous courses for the computer forensic arena, specializing in the field of wireless forensics as well as mobile technologies. Ms Schroader is the CEO of Paraben Corporation. Ms Schroader is involved in many different computer investigation organizations including The Institute of Computer Forensic Professionals (ICFP), HTCIA, CFTT, and FLETC.*

Tyler Cohen *is an instructor and developer for the Department of Defense Cyber Crime Center. Her specialties are digital forensics, network intrusions, and conducting forensic exams with the iPod and other alternative media devices. She presents her expertise at various conferences all over the country some of which include the Department of Defense Cyber Crime Conference, International High Technology Crime Investigation Association and the California District Attorney's Cyber Crime Conference.*

A Tale of Two Proxies
SensePost

During this presentation SensePost will discuss and demonstrate two pieces of new technology—the Suru WebProxy and the SP_LR Generic network proxy.

The Suru web proxy is an inline web proxy (the likes of Paros, @stake webproxy and Webscarab) and offers the analyst unparalleled functionality. Are the days of the web proxy counted? Is there really room for another web proxy? Come to their presentation and see what happened when the guys at SensePost decided to develop a proxy with punch.

SP_LR is a generic proxy framework that can be used for malware analysis, fuzzing or just the terminally curious. Its a tiny, generic proxy built on open-source tools with extensibility in mind at a low low price (GPL - Free as in beer).

Both proxies serve distinct masters and will be valuable tools in any analysts arsenal.

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". 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. Haroon doesnt drink tea or smoke camels.*

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

How the FBI uses NLP on YOU!
Brad Smith, RN, CISSP, Computer Institute of the, Rockies

This session will reveal to you how the FBI uses Neuro-Linguistic Programming (NLP) during interview and interrogation sessions. Gaining cooperation with special speech and word changes, Clues to help determine whether clients are lying or remembering and the traditional "Cop Stop technique" will all be revealed and practiced by attendees. Seldom taught outside the law or medical community, you'll be instructed in and actual practice techniques, just like the Feds do. While you may not be able to stop leaking information to the specially trained professional, you'll now see the extra information other are giving off. Come prepared to talk to others and learn invaluable skills that can C.Y.A.

Brad Smith, *RN, BS-Psych, CISSP has utilized social engineering in Emergency rooms to defuse medical crisis for many years. He has taught Neuro-Linguistic Programming to healthcare, law enforcement and security professionals and now helps educate everyone on the reality of social engineering and its exploits.*

The Jericho Forum and Challenge
Presenter: Paul Simmonds, CISO, ICI
Judges: Pamela Fusco, EVP, CitiGroup
David Mortman, former CISO, Siebel
Henry Teng, CISO, Philips

In the first half of this session, Paul Simmonds will present on behalf of the Jericho Forum taking participants through the initial problem statement and what people need to go away and start implementing. Topics will include:

1. De-perimeterization - the business imperative
2. From protocols to accessing the web - the technical issues
3. What should be implemented today - current and near term solutions
4. Planning for tomorrow - future solutions and roadmap

The second half on this session will focus on the Jericho Challenge, the format, the rules, the judging format and the prizes followed by a Q&A. The aim with the Jericho Form Challenge is to develop a "technology demonstrator" with a full year from start to finish. The competition is based on a typical business environment with at least one business application, one legacy application, typical business usage (Web, E-mail and Word Processing) using at least one "office" PC and one laptop. The finals and judging will occur in 2007 at DEFCON.

Paul Simmonds *joined ICI in 2001 when he was recruited to head up Information Security for ICI, working for the CIO Office in London. Prior to joining ICI he spent a short time with a high security European web hosting company as Head of Information Security, and prior to that seven years with Motorola, again in a global information security role. In his career he has worked with many external agencies, and has also been directly involved in two successful criminal prosecutions, giving evidence in one case.*

Paul came to the Information Security field from a background in IT Systems Implementation and consultancy during which he wrote and implemented one of the UK's first web sites. Paul was voted 36th in the 2004 list of the top 50 most powerful people in networking, by the US publication Network World Fusion, for his work with the Jericho Forum.

Pamela Fusco *is EVP and Head of CTI Global Security for CitiGroup. She was previously Executive Global Information Security Professional for Merck & CO., Inc. Pamela has accumulated over 19 years of substantial experience within the Security Industry. Her extensive background and expertise expand globally encompassing all facets of security inclusive of logical, physical, personal, facilities, systems, networks, wireless, and forensic investigations.*

David Mortman *is former CISO for Siebel Systems, Inc. where he and his team were responsible for Siebel Systems' worldwide IT security infrastructure, both internal and external. He also worked closely with Siebel's product groups and the company's physical security team and was leading up Siebel's product security and privacy efforts. Previously, Mr. Mortman was Manager of IT Security at Network Associates, where, in addition to managing data security, he deployed and tested all of NAI's security products before they were released to customers. A CISSP, member of USENIX/SAGE and ISSA, and an invited speaker at RSA 2002 and 2005 security conferences, Mr. Mortman has also been a panelist at InfoSecurity 2003, Black Hat 2004 and 2005 as well as Defcon 2005. He sits on a variety of advisory boards including Qualys, Teros, and Sygate amongst others. Mr. Mortman holds a BS in Chemistry from the University of Chicago*

Henry Teng *is the Enterprise Security compliance officer, Senior Director for Philips International B.V. He is currently based in The Netherlands. Henry is responsible for the global Enterprise Security Compliance Management Program including information security and IT security for Philips in the Americas, Europe, and Asia Pacific. Philips International has annual revenue of about $36 billion and a worldwide employee population of 126,000.*

Henry has over nineteen years of IT security, information security, risk and compliance management experience for fortune 500 companies ranging from financial services, e-commerce, to electronics manufacturing. He is the author of three patents on security related areas granted by the U.S. Patent Office.

Prior to Philips Henry worked for a number of large enterprises such as eBay as their chief of Information Security, for Charles Schwab as their Managing Director of Security Engineering & Design, and for KPMG LLP in the Risk & Advisory Services.

Henry served as a Board member for the Information Systems Security Association (ISSA) Silicon Valley Chapter for two years. He was also one of the founding members of an industry consortium against distributed denial of service (DDoS) attacks and served as its chairperson from 2000 to 2002.

Hunting for Metamorphic Engines

Mark Stamp, Assistant Professor, Department of Computer Science, San Jose State University

Wing H. Wong, Student, San Jose State University

Metamorphism has been touted as a way to generate undetectable viruses and worms, and it has also been suggested as a potential security-enhancing technique. Today metamorphic virus construction kits are readily available on the Internet. A visit to the VX Heavens reveals more than 150 generators and engines to choose from in the category of "Worm/Virus Creation Tools". The purpose of a metamorphic generator is to create multiple instances of a virus which are sufficiently different from each other so as to avoid detection. How effective are these metamorphic engines? How different are the morphed variants? Is it possible to detect metamorphic viruses and worms?

We analyze several metamorphic engines (include MPCGEN Mass Code Generator, G2, NGVCK, and VCL32). In each case, we precisely measure the similarity of different instances of the morphed code. We show that the morphing abilities of these engines varies widely. We also show that, ironically, the metamorphic viruses we tested are easy to distinguish from normal code, regardless of the effectiveness of the morphing. Our results indicate that, in practice, it may be more difficult to effectively use metamorphism as a means to avoid detection than is generally believed.

Mark Stamp *can neither confirm nor deny that he spent 7 years as a National Security Agency cryptanalyst. However, he can confirm that he spent 2 years as Chief Cryptologic Scientist at a small Silicon Valley startup, where he helped develop a digital rights management (DRM) system. For the past 4 years he has been Assistant Professor in the Department of Computer Science at San Jose State University, where he teaches courses in information security, networking, and cryptography. He recently published a textbook, Information Security: Principles and Practice (Wiley Interscience, 2006) and he has just completed a second textbook, Applied Cryptanalysis.*

Wing H. Wong *is a graduate student at San Jose State University. Her research interests include network security and bioinformatics.*

OllyBone: Semi-Automatic Unpacking on IA-32

Joe Stewart, Senior Security Researcher, LURHQ

The amount of new malware being developed has increased at a staggering rate over the last couple of years. At the same time, executable packing technology has grown to provide malware authors with a myriad of choices in how they pack their malware to evade detection and analysis. This presents a growing problem to analysts who lack the time to learn how each packer works and can be unpacked, but still need to be able to quickly handle anything that comes their way.

There are three conventional approaches to automatic unpacking, including unpacking by emulation (very difficult to write 100% compatible to the platform and therefore tools that are closely held by their authors), unpacking by memory dump (not reliable and, will also corrupt variables with their post-initialization values), and finally, writing a specific unpacking engine for each packer based on reverse-engineering the packer code (also a huge undertaking to have enough coverage, also a cat-and-mouse game).

In this presentation I will demonstrate a semi-automatic approach to unpacking malware that bridges the gap between highly-skilled manual unpacking and speedy but costly automatic unpacking. By leveraging certain aspects of the i386 architecture we can unpack code from a great deal of packers to the OEP without emulation or specific knowledge of the packing algorithm.

Joe Stewart, *GCIH - Senior Security Researcher with LURHQ, a leading Managed Security Services Provider. In this role he researches unusual Internet activity to discover emerging threats, new attack techniques and the latest malicious code. He is a SANS Global Information Assurance Certified Incident Handler (GCIH) and has been in the information security field for six years. He is a frequent commentator on security issues for leading media organizations such as The New York Times, MSNBC, Washington Post, Bloomberg and others. Additionally, Joe has published numerous security research papers on Sobig, Migmaf, Sinit, Phatbot, BlackWorm, Cryzip and other cyber-threats and attack techniques. Joe is the author of software projects Fess, Mumsie, and Truman as well as numerous OllyDbg plugins including OllyPerl.*

Beyond Social Engineering: Tools for Reinventing Yourself
Richard Thieme, Thiemeworks

Managing multiple modular identities is not a trivial task. But that's what the technologies and politics of Now demand. These tools will enable you to create personas at a deep level, then link them into a seamless life.

Richard Thieme is a business consultant, writer, and professional speaker focused on "life on the edge," in particular the human dimension of technology and work. He is a contributing editor for Information Security Magazine. Speaking/consulting clients include: GE Medical Systems; Los Alamos National Laboratory; Apache Con; Microsoft; Network Flight Recorder; System Planning Corporation (SPC); InfraGard; Firstar Bank; Financial Services - Information Sharing and Analysis Center (FS-ISAC); Psynapse/Center for the Advancement of Intelligent Systems; Cypress Systems; Assn. for Investment Management and Research (AIMR); Alliant Energy; Wisconsin Electric; UOP; Ajilon; OmniTech; Strong Capital Management; MAPICS; Influent Technology Group; FBI; US Department of the Treasury; the Attorney General of the State of Wisconsin; and the Technology, Literacy and Culture Distinguished Speakers Series of the University of Texas.

Advanced File System Hiding and Detection
Irby Thompson, Senior Security Engineer, Advanced Technology Laboratories, Lockheed Martin
Mathew Monroe, Senior Security Engineer, Advanced Technology Laboratories, Lockheed Martin

The ability to both conceal and detect hidden data on the hard drive of a compromised computer represents an important arms-race between hackers and forensic analysts. While rootkits and other kernel manipulation tools make hiding on live systems fairly easy, the trick of hiding data from forensic tools and offline drive analysis is much more difficult. In this presentation, we will review traditional data hiding techniques, examine their strengths and weaknesses, and then explore more advanced methods of data hiding which go beyond the detection capabilities of current forensics tools. Further attention will be given to enabling transparent access to hidden file systems while also minimizing detection, ensuring data confidentiality, and providing robustness against corruption. The culmination of our research will be demonstrated in an advanced data hiding methodology and corresponding forensic detection utility.

***Irby Thompson** is currently a Senior Security Engineer for the Advanced Technology Laboratories of Lockheed Martin. His early interest in computer security led to a career in network and host security with a focus on operating system security and applied cryptography. Irby's past experience includes the design and development of a secure email system including features such as guaranteed read-receipts, message expiration, one-time read, and un-send capabilities.*

***Mathew Monroe** is an accomplished developer specializing in embedded systems and computer security. In addition, Mathew has experience designing and implementing high performance distributed file systems and applications. He is currently a Senior Security Engineer at the Lockheed Martin Advanced Technology Laboratories. Prior to this post he implemented, deployed, and tested Lustre file systems on Lawrence Livermore National Laboratory's MCR and ACL clusters and Pacific Northwest National Laboratory's rx2800 cluster. In addition, Mathew designed and implemented firmware and low level file system code for network attached storage devices at Spinnaker Networks (now Network Appliances).*

Things That Go "Bump" in the night: An Analysis of Current and Emerging Threats to Physical Security
Marc Weber Tobias, Investigative Law Offices, Security.org
Matt Fiddler, Security Consultant - Security.org

Although there has been a significant amount of attention paid to the topic of late, there are complexities that must be understood to accurately gauge the impact of "Bumping Locks" on physical security. This talk will explore the vulnerabilities and exposures of virtually all pin-tumbler locks, highlighting the legal issues surrounding the possession and use of bump-keys and bumping implements. Case examples and demonstrations detailing a major security flaw and vulnerability in locks used by the

federal government and a private sector corporation that affect millions of users will be presented.

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

Mr. Tobias is the author of the 1400 page textbook and multimedia collection "Locks, Safes, and Security: An International Police Reference". He consults on lock security and his law firm handles investigations for government and private clients.

Matt Fiddler *leads a Threat Management Team for a large Fortune 100 Company. Mr. Fiddler's research into lock bypass techniques have resulted in several public disclosures of critical lock design flaws. Mr. Fiddler began his career as an Intelligence Analyst with the United States Marine Corps. Currently Mr. Fiddler is the Connecticut Chapter President and active Board Member of Locksport International.*

Kiosk Security

Peleus Uhley, Principal Security Consultant, Symantec Professional Services

Kiosks are being deployed in an increasing number of locations including supermarkets, banks and airports. Providing public computer access from machines connected to your internal network is one of the most challenging IT problems. Traditionally, an anonymous user with local access to a machine that can talk to the Internet and the internal network is an administrator's nightmare. Therefore the techniques to secure these machines must go far beyond the procedures for a normal desktop environment. Often times these devices are deployed on the same network as the store's cash registers introducing PCI compliance issues. Relying on store employees to monitor for kiosk abuse is not an option. This discussion will focus on the security issues surrounding the deployment of Windows-based kiosks. Deployment strategies, application security design, PCI compliance issues, known attack methods and common security tools will be covered.

Peleus Uhley *is a Principal Security Consultant with the Symantec Professional Services team where he performs wireless, network and application penetration testing for clients. Several of his recent engagements have covered assessing kiosk security for retailers. As part of the Advisory Services team, Peleus also serves an Attack and Penetration Center of Excellence lead helping to develop penetration testing services and coordinate knowledge development and tools for Symantec consultants. Prior to being a security consultant, he was the lead developer for the online privacy company, Anonymizer. Peleus has also given talks and authored a white paper on web browser security.*

Hacking Malware: Offense Is the New Defense

Valsmith, Co-Founder, Offensive Computing

Danny Quist, co-founder Offensive Computing

The proliferation of malware is a serious problem, which grows in sophistication and complexity every day, but with this growth, comes a price. The price that malware pays for advanced features and sophistication is increased vulnerability to attack. Malware is a system, just like an OS or application. Systems employ security mechanisms to defend themselves and also suffer from vulnerabilities which can be exploited. Malware is no different.

Malware authors are employing constantly evolving techniques including binary obfuscation, anti-debugging and anti-analysis, and built in attacks against protection systems such as anti-virus software and firewalls.

This presentation will dig into these techniques and explain the basics. The idea of an open source malware analysis and research community will be explored. All the things the Anti-Virus vendors don't want you to know will be discussed. Methods for bypassing malware's security systems will be presented. These methods include detecting and defeating packers/encoders, hiding the debugger from the malware, and protecting analysis virtual machines. We will hack the malware.

Valsmith *has been involved in the computer security community and industry for over ten years. He currently works as a professional security researcher on problems for both the government and private sectors. He specializes in penetration testing, reverse engineering*

and malware research. Valsmith is a member of the Cult of the Dead Cow NSF. He also works on the Metasploit Project development team as well as other vulnerability development efforts. Most recently Valsmith founded Offensive Computing, a public, open source malware research project.

***Danny Quist (Chamuco)** is a computer security professional who has been interested in malware and hacking ever since the Michelangelo computer virus was released many years ago. He has written several defensive systems to mitigate virus attacks on networks and developed a generic network quarantine technology. He consults both with both private and public sectors on system and network security projects. His interests include malware defense, reverse engineering, exploitation methods, virtual machines, and automatic classification systems.*

DNS Amplification Attacks

Randal Vaughn, Professor, Informatio Systems, Baylor University
Gadi Evron

This paper outlines a Distributed Denial of Service (DDoS) attack which abuses open recursive Domain Name System (DNS) name servers using spoofed UDP packets.

Our study is based on packet captures and logs from attacks reported to have a volume of 2.8Gbps. We study this data in order to further understand the basics of the reported recursive name server amplification attacks which are also known as DNS amplification or DNS reflector attacks. One of the networks under attack, Sharktech, indicated some attacks have reached as high as 10Gbps and used as many as 140,000 exploited name servers. In addition to the increase in the response packet size, the large UDP packets create IP protocol fragments. Several other responses also contribute to the overall effectiveness of these attacks.

The risks involved with the recursive name server feature, as well as those of packet spoofing are well known, yet have been treated more as a theoretical issue. The attack under study was anticipated as early as 2002 (gnupg 2002). Earlier attacks using queries to non-authoritative servers were for a reflection attack using MX records (Mirkovic, Dietrich, Dittrich. and Reiher). To our knowledge, this is the first documentation of a new form of a recursive name server reflection attack designed to use the significantly larger data amplification available from the extended capabilities of extended DNS standards. In addition to this attack technique, recursion can be leveraged for other uses such as theft of DNS resources (CERT UNI-Stuttgart 2003).

***Randal Vaughn** teaches a variety of courses in Information Systems. Vaughn is a widely quoted expert in the areas of cyber warfare, cyber defense, and internet threat metrics and reporting. He is on the Board of Advisors for MI5 Security and an Academic associate for the AntiPhishingWorkingGroup. He is a member of Educause, the Society for Information Management (SIM), and the Association for Computing Machinery (ACM). His work has been published in several mathematics publications and he has authored white papers such as "Using PowWow in the Academic Environment" for Tribal Voice. Previously, Vaughn worked at Mobil Exploration and Producing Services, Inc. as a computer analyst for seismic processing support. Prior to that, he was the lead designer for Vought Aircraft's Group Technology Support Software—a component of the U.S. Air Force's Integrated Computer Aided Manufacturing project. He also served in the U.S. Air Force as a project engineer and database administrator. Vaughn's operating system experience includes legacy mainframe operating systems, Microsoft' Windows', Linux, and Apple' Mac' OS and Mac OS X operating systems.*

Malware Repository Requirements

Paul Vixie, President, ISC
David Dagon, PhD Student, GATECH

We describe requirements for a malware collection repository. The repository serves as a clearing house for malware samples, as well as analysis provided by members of the clearing house.

We discuss how malware authors are aware of, and actively exploit inherent inefficiencies in the current generation of competitive, closed malware collections. We demonstrate how, by illuminating AV sensors, and by using frequent updates, malware authors can keep their victims within a perpetual zero-day window.

The are numerous cooperative malware repositories created to address problems in private collections. After exploring the policy trade-offs, we describe our own solution. Features include automated unpacking of samples, data mining of packed samples, static and dynamic analysis, and selected network trace files.

Paul Vixie *holds the record for "most CERT advisories due to a single author" which came primarily from his years hacking on BIND4 and BIND8. Later on he cut off the oxygen supply to his brain by wearing a necktie for AboveNet, MFN, and PAIX. At the moment he is President at ISC where his primary duty is to sign paychecks for the people who bring you BIND9 and F.ROOT-SERVERS.NET. He is also an occasional critic of just about everything (the blog: FM.VIX.COM).*

David Dagon *is a PhD student in the College of Computing at Georgia Institute of Technology. His area of research includes network security, BSD kernel hacking, honeynets, and malware analysis. He has written extensively about malware, including modelling botnet propagation using time zones and the KarstNet active sinkhole. We describe requirements for a malware collection repository. The repository serves as a clearing house for malware samples, as well as analysis provided by members of the clearing house.*

The Plausible Deniability Toolkit
weasel, Nomad Mobile Research Centre
simple nomad, Nomad Mobile Research Centre

The Plausible Deniability Toolkit is a collection of processes and tools designed to protect its users from invasions of privacy and infringement of civil rights by oppresive organizations and governments. The foundation for this toolkit is the result of anti-forensics gap analysis and the need for fabrication of evidence. Certainly most of these techniques have been in use by child pornography rings and various governmental TLA's, but we intend to bring them forward for more legitimate usages, such as protecting civil activist and whistleblowers.

This presentation will consist of a walkthough of the gaps left behind by anti-forensics techniques, as well as describe the technologies and techniques used by the toolkit. We will aslo cover live demonstrations of the tools and their uses as well as allow plenty of flexibility for audience interaction.

And if there it time left at the end, we will do a live hacking of Jeff Moss' bank accounts.

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

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

UNCLASSIFIED Information Sharing with Non-Traditional Partners
Dr. Linton Wells II, Assistant Secretary of Defense for Networks and Information Integration / CIO

Experience from domestic and foreign humanitarian assistance and disaster relief (HADR) operations shows that shared situational awareness and the information systems that support it are the critical enablers of all other functions in such situations. They are not merely technical adjuncts to the delivery of food, water and shelter. Federal Agencies can respond better to disasters (both domestic and international) by sharing unclassified information effectively with state, local and tribal governments, non-governmental organizations, and relief entities. DoD often refers to these as "non-traditional partners." Besides sharing situational awareness, decision-makers also must exchange ideas for solving emergent problems and convert decisions into action. These capabilities need to be in place within hours after the beginning of a crisis. Success will require new cultures of unclassified information sharing; not just within DoD, but also with the non-traditional partners that form the backbone of domestic and international disaster response.

Dr. Linton Wells II *serves as the Principal Deputy Assistant Secretary of Defense (Networks and Information Integration). He resumed these duties on November 14, 2005 after serving as the Acting Assistant Secretary and DoD Chief Information Officer from March 8, 2004. He became the Principal Deputy Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on August 20, 1998 which became Networks and Information Integration in 2003. Prior to this assignment, he had served in the Office of the Under Secretary of Defense (Policy) from 1991 to 1998, most recently as the Deputy Under Secretary of Defense (Policy Support).*

In twenty-six years of naval service, Dr. Wells served in a variety of surface ships, including command of a destroyer squadron and guided missile destroyer. In addition, he acquired a wide range of experience in operations analysis; Pacific, Indian Ocean and Middle East affairs; C3I; and special access program oversight.

Dr. Wells has written widely on security studies in English and Japanese journals. He co-authored Japanese Cruisers of the Pacific War, which was published in 1997. His hobbies include history, the relationship between policy and technology, scuba diving, and flying.

Abuse and the Global Infection Rate

Rick Wesson, CEO Support Intelligence, LLC

Detecting global abuse patterns with realtime black lists, spamtraps and honey pots. Understanding what your network is doing to the rest of the community is difficult, we discuss how to use our tools to understand how your network is abusing other networks and show graphs and stats of trends globably and within the us.

Rick Wesson *has worked in the IETF and ICANN on DNS, whois, and Registry and Registrar protocols; Served for 4 years as the CTO of the Registrars Constituency in the GNSO/ICANN framework and 2 years on the ICANN security and Stability Committee.*

The National Collegiate Cyber Defense Competition

Greg White, Director, Center for Infrastructure Assurance and Security
Kevin Archer, Senior Security Engineer, Center for Infrastructure Assurance and Security

Security competitions have been of interest to many individuals for a number of years. The popularity of the annual DEFCON competition demonstrates the level of interest in these events. This talk will discuss the creation of the National Collegiate Cyber Defense Competition which was held in April 2006. A brief history covering the development of this competition will be covered as well as a discussion of the event itself. The results of the competition will be presented as well as the lessons learned from it and the plans to hold similar future events. A description of the hardware and software used as well as the network configuration and red team composition and activity will also be addressed.

Dr. Gregory White *has been involved in computer and network security since 1986. He spent 19 years on active duty with the Air Force and is currently in the Air Force Reserves assigned to the Pentagon. He is currently the Director for the Center for Infrastructure Assurance and Security and is an Associate Professor of Computer Science at The University of Texas at San Antonio (UTSA).*

Dr. White has been involved in security instruction for a number of years. He taught at the U.S. Air Force Academy for seven years where he developed and taught two courses on Computer Security and Information Warfare. For the last two years, he has been heavily involved in developing and promoting the idea of conducting an annual collegiate cyber security competition.

Dr. White has written and presented numerous articles and conference papers on security. He is also the co-author for six textbooks on computer and network security and has written chapters included in two other security books.

Corporate Network Spying

Andrew Whitaker, CISSP

Learn to Spy on Corporate Network Traffic. After attending this talk, you will learn how to perform targeted packet sniffing to capture web, e-mail, chat conversations, VoIP, and file transfer traffic. Many tools are covered, including Effetech, MSN Protocol Analyzer, Ethereal filters, URLSnarf, FileSnarf, ACE, Cain and Abel, and others.

Andrew Whitaker *is the Director of Enterprise Security for InfoSec Academy, a global leader in accelerated information security training. In his position, Andrew travels throughout the United States speaking at conferences and teaching courses on penetration testing and vulnerability assessments. He is a contributor to several articles and books including being the co-author of the book "Penetration Testing and Network Defense" (Cisco Press, 2005). Andrew performs numerous penetration tests for organizations each year, helping companies improve their information security. Along with a Master's degree in computer science, Andrew holds the following certifications: CCSP, CEH, CEI, CCNP, INFOSEC, MCSE, CNE, CCNA, CCDA, A+, Security+, Network+, and CTP.*

Blackjacking - owning the Enterprise via the Blackberry
x30n

Research in Motion's Blackberry technology has quickly become the defacto standard for executives and technical personnel alike to maintain unteathered remote access to critical data. Often regarded as inherently secure, most administrators deploy this solution without a full understanding of the technology or risks involved.

This presentation will demonstrate how an attacker could utilize many typical corporate blackberry deployments to directly attack machines on the internal network—behind your perimiter defenses! The tools and source code presented will be available for attendees. Techniques for reducing the risks associated with this technology will also be presented.

This talk is a must see for anyone who has deployed or is planning on deploying the Blackberry solution within their network. Whether you are an administrator, CIO, security officer, or user, you can't afford not to understand the risks associated with this technology.

x30n *has over 8 years of experience in software and network security. His expertise and industry experience includes software engineering, vulnerability research, exploit development, risk managment, penetration testing, source code auditing, reverse engineering, forensic analysis, and network analysis as well as many other niche areas within the information security industry.*

x30n is also a core member as well as current team captain of Digital Revelation, the notorious research group that has taken 1st place in Defcon's Capture the Flag competition twice.

Panel: Ask EFF: The Year in Digital Civil Liberties
Cindy Cohn, EFF Legal Director
Kevin Bankston, EFF Staff Attorney
Kurt Opsahl, EFF Staff Attorney
Jason Schultz, EFF Staff Attorneys
Danny O'Brien, EFF Activism Coordinator
Seth Schoen, EFF Staff Technologist

Get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This session will include updates on current EFF issues such as NSA wiretapping, cellphone tracking by the government, bloggers' rights and online journalism, the Sony rootkit scandal, Hollywood's latest attempts to control technology development, and more. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.

Cindy Cohn *is the Legal Director for the Electronic Frontier Foundation as well as its General Counsel. She is responsible for overseeing the EFF's overall legal strategy and supervising EFF's 7 staff attorneys. Outside the Courts, Ms. Cohn has testified before Congress, been featured in the New York Times, San Francisco Chronicle and elsewhere for her work on cyberspace issues, interviewed on the BBC, NPR, CNN, CBS News and the Newshour, Economist, Wall Street Journal, Washington Post and many other online and offline media outlets.*

Kevin Bankston, *an EFF staff attorney specializing in free speech and privacy law, was EFF's Equal Justice Works/Bruce J. Ennis Fellow for 2003-05. His fellowship project focused on the impact of post-9/11 anti-terrorism laws and surveillance initiatives on online privacy and free expression. Before joining EFF, Kevin was the Justice William J. Brennan First Amendment Fellow for the American Civil Liberties Union in New York City. At the ACLU, Kevin*

litigated Internet-related free speech cases, including First Amendment challenges to both the Digital Millennium Copyright Act (Edelman v. N2H2, Inc.) and a federal statute regulating Internet speech in public libraries (American Library Association v. U.S.).

***Danny O'Brien** is the Activist Coordinator for the EFF. His job is to help our membership in making their voice heard: in government and regulatory circles, in the marketplace, and with the wider public. Danny has documented and fought for digital rights in the UK for over a decade, where he also assisted in building tools of open democracy like Fax Your MP.*

***Kurt Opsahl** is a Staff Attorney with the Electronic Frontier Foundation focusing on civil liberties, free speech and privacy law. Before joining EFF, Opsahl worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters, including working on Kelly v. Arribasoft, MGM v. Grokster and CoStar v. LoopNet. For his work responding to government subpoenas, Opsahl is proud to have been called a "rabid dog" by the Department of Justice. Prior to Perkins, Opsahl was a research fellow to Professor Pamela Samuelson at the U.C. Berkeley School of Information Management & Systems. Opsahl co-authored "Electronic Media and Privacy Law Handbook.*

***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. While at Linuxcare, Schoen helped create the Linuxcare Bootable Business Card CD-ROM.*

***Jason Schultz** is a Staff Attorney specializing in intellectual property and reverse engineering. He currently leads EFF's Patent Busting Project. Jason also teaches graduate classes on Cyberlaw at UC Berkeley's Boalt Hall School of Law and School of Information. Prior to joining EFF, Schultz worked at the law firm of Fish & Richardson P.C. While at F&R, he co-authored an amicus brief on behalf of the Internet Archive, Prelinger Archives, and Project Gutenberg in support of Eric Eldred's challenge to the Sonny Bono Copyright Term Extension Act. During law school, Schultz served as Managing Editor of the Berkeley Technology Law Journal and helped found the Samuelson Clinic, the first legal clinic in the country to focus on high tech policy issues and the public interest.*

PANEL: EFF v. AT&T: Your World, Delivered (to the NSA)
Cindy Cohn, EFF Legal Director
Kevin Bankston, EFF Staff Attorney
Kurt Opsahl, EFF Staff Attorney
Jason Schultz, EFF Staff Attorneys

If you want to know how the National Security Agency and telecommunications companies are conspiring to invade your privacy, this is the panel for you. The Electroni Frontier Foundation (EFF) is currently suing AT&T for collaborating with the NSA in its massive and illegal program to wiretap and data-mine Americans' phone and internet communications. Come learn about the legal and technical issues surrounding the NSA surveillance program, find out what Congress is (or isn't) doing about it, and get an up-to-the-minute update from the EFF lawyers on their lawsuit and other NSA-related court cases across the country.

Panel: Internet Wars 2006
Gadi Evron
Mudge (directing the panel)
Paul Vixie
Dan Kaminsky
Randy Vaughn
Dan Hubbard, Websense
Supervisory Special Agent Thomas X. Grasso, Jr., Federal Bureau of Investigation

In this panel session we will begin with a short introductory presentation from Gadi Evron on the latest technologies and operations by the Bad Guys and the Good Guys. What's going on with Internet operations, global routing, botnets, extortion, phishing and the annual revenue the mafia is getting from it. The panel session itself will be hosted by mudge. The members will accept questions on any subject related to the topic at hand, and discuss it openly in regard to what's being done and what we can expect in the future—both from the Bad Guys and the Good Guys.

***Dan Hubbard** is the VP of Security Research at Websense. He is responsible for all things security at Websense, including managing the Websense Security Labs that researches, analyzes, and reverse engineers malicious code, analyzes security trends, and provides research on malicious Websites and network protocols. Hubbard also defines security-related product features. He is the pioneer behind Websense's Web filtering database that supports its Security Group. Hubbard also acts as the company's security spokesperson.*

PANEL: Meet the Feds: OODA Loop and the Science of Security
Jason Beckett, New South Wales Police in Sydney Australia
James Christy, DC3
SA Andy Fried, Internal Revenue Service (IRS)
Mike Jacobs, SRA
Rich Marshall, National Security Agency (NSA)
Ken Privette, USPS OIG
Keith Rhodes, CTO, Government Accountability Office (GAO)
Dave Thomas, FBI
Bob Hopper, National White Collar Crime Center
Jon Lee, NCIS
Hilary Stanhope, CIA
Tim Fowler, Marine Special Agent, Naval Criminal Investigative Service (NCIS)

The OODA Loop theory was conceived by Col John Boyd, AF fighter pilot. He believed that a pilot in a lethal engagement that could Observe, Orient, Decide, and Act (OODA) before his adversary had a better chance to survive. He considered air combat an art rather than a science. John Boyd proved air combat could be codified; for every maneuver there is a series of counter maneuvers and there is a counter to every counter. Today, successful fighter pilots study every option open to their adversary and how to respond. This panel's focus is on the government efforts to try to get inside the cyber adversary's OODA Loop and survive another type of potential cyber lethal engagement.

***Supervisory Special Agent Jim Christy,** is the Director of the Defense Cyber Crime Institute (DCCI), Defense Cyber Crime Center (DC3). The DCCI is responsible for the research & development and test & evaluation of forensic and investigative tools for the DoD Law Enforcement and Counterintelligence organizations. The Institute is also charged with intelligence analysis, outreach, and policy for DC3. Jim is an Air Force Office of Special Investigations, Computer Crime Investigator. SA Christy has been a computer crime investigator for over 20 years.*

***Jason Beckett** is the Director of the State Electronic Evidence Branch of the Special Services Group for the New South Wales Police in Sydney Australia. A former Inspector with the Special Services Group before moving to the corporate world as the Director of forensics for a multinational consultancy firm. In 2003 he was invited back to the New South Wales Police Force to establish Australia's largest forensic computing laboratory. Jason has more than a decade of experience in Electronic Evidence and forensic computing.*

***Michael Jacobs** joined SRA in October 2002 as a Senior Advisor following his retirement from the Federal Government after 38 years of service. In March 2003 he was appointed Director of SRA's Cyber and National Security Program. Prior to SRA, Mr. Jacobs was the Information Assurance (IA) Director at the National Security Agency (NSA). Under his leadership, NSA began implementing an Information Assurance strategy to protect the Defense Information Infrastructure and as appropriate, the National Information Infrastructure.*

Mr. Jacobs had a long and distinguished career at the National Security Agency where he served in key management positions in both the Intelligence and IA mission areas. He served as the Deputy Associate Director for Operations, Military Support where he was responsible for developing a single, coherent military support strategy for NSA. During his 38 years of NSA service, Jacobs was a leader in Information Systems Security production and control, policy and doctrine and customer relations. He has testified before Congress on defense issues and has spoken widely on topics ranging from IA to cultural diversity.

***Ken Privette** presently works as the Special Agent in Charge of the Computer Crimes Unit (CCU) at the USPS Office of Inspector General. His unit conducts computer intrusion investigations and provides computer forensics support to a force of over 450 agents who conduct fraud investigations for the U. S. Postal Service. Ken spent most of his professional life as a Special Agent with the Naval Criminal Investigative Service both overseas and*

state-side where he conducted investigations involving computer crime, terrorism, and counterintelligence matters, in adition to an assignment with the Defense Information Systems Agency Computer Emergency Response Team.

***Keith Rhodes** is currently the CTO of the U. S. GAO and Director of the Center for Technology & Engineering. Mr. Rhodes has been the senior advisor on a range of assignments covering continuity of government & operations, export control, computer security & privacy, e-commerce & e-government, voting systems, and various unconventional weapons systems. Before joining GAO, he was a supervisory scientist leading weapons and intelligence programs at the Lawrence Livermore National Laboratory.*

***David A. Thomas** was designated a Special Agent of the FBI in 1989. After completing more than a dozen years of supervisory and leadership roles in areas such as violent crime, domestic terrorism, and national infrastructure Protection, Mr. Thomas was appointed Chief of the Cyber Division's Criminal Computer Intrusion Unit in 2001. In July 2004, Mr. Thomas was promoted to the position of Chief of Counterterrorism/Counterintelligence and Criminal computer intrusion investigations. Additionally, he is responsible for development of the FBI's Cyber Intelligence Unit and Cyber Action Teams, which deploy domestically and internationally in response to major cyber events.*

***Tim Fowler** is an active duty Marine Special Agent who has worked as a Cyber Agent for the NCIS Cyber Department in Washington, DC, for the last six years. Tim has 19 years of active duty service in the U.S. Marine Corps working in the fields of military police, polygraph, criminal investigations and computer crime investigations and operations. While working as a Cyber Agent for NCIS, Tim specializes in conducting criminal, counterintelligence and counter-terrorism computer crime investigations and operations. Tim also has extensive knowledge and experience conducting media exploitation operations in hostile environments.*

SLOGAN CONTEST

WINNER:

Mad Jester

Society doesn't understand me, and technology fears me.

RUNNERS UP:

v1s1on

In silence I lay, for that fateful day. Ø-day!

Addictus

Subversion Illuminated

Strom Carlson

DefCon: Where goons stay sober so you don't have to!

T-SHIRT ARTWORK

AN ARMY OF ON3



WINNER: Haxor

VENDORS

VENDOR AREA HOURS ARE 10:00 - 19:00

Blacklisted 411

MECO

Shadowvex

Boblbee

MediaArchives.com

Sound of Knowledge

BreakPoint Books

Ninja Networks

Tim Huynh

EFF

Overdose

UAT

E-Teknet

RainbowTables.net

Unix Surplus

Irvine Underground

Root Compromise

WarDrivingWorld.Com

Jinx

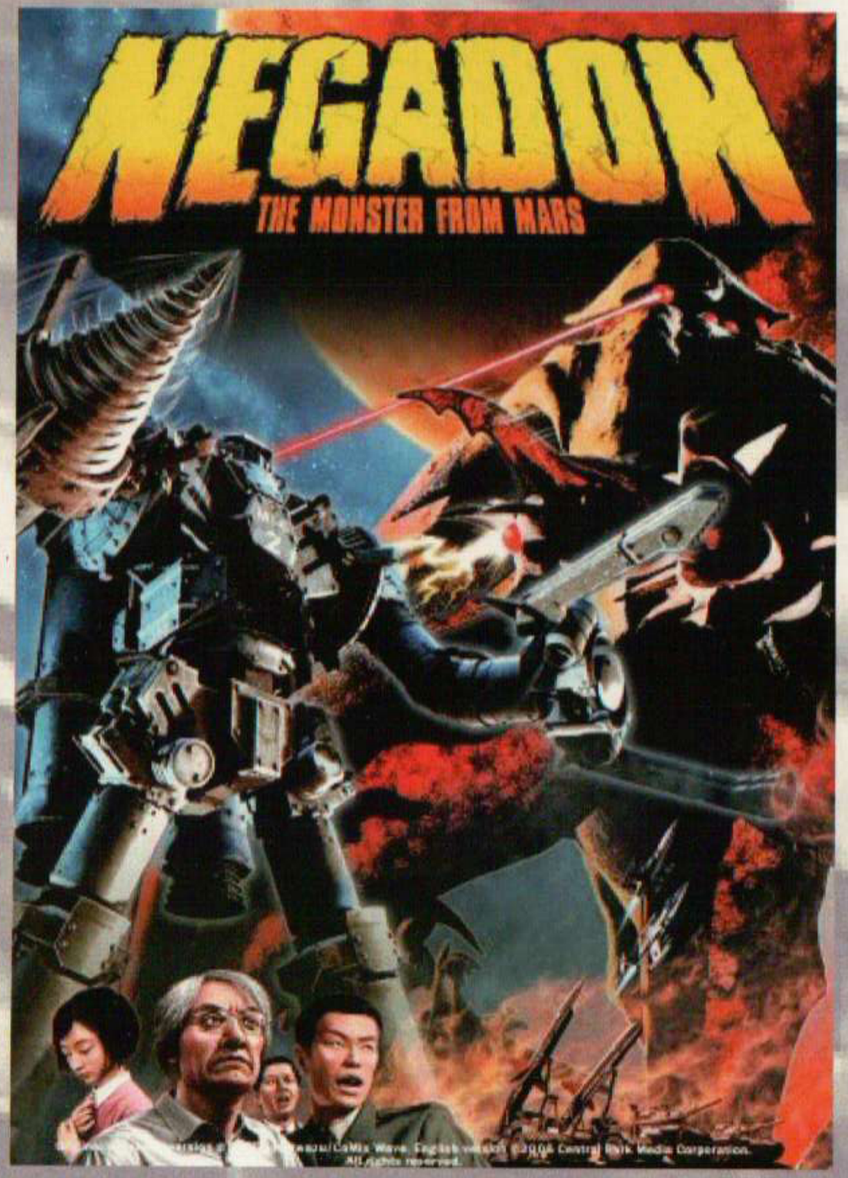
J!NX: FIND OFFICIAL DC CLOTHING AND MERCHANDISE AT J!NX HACKWEAR

DAY 1
FRIDAY
AUGUST 4

	TRACK ONE ROYALE PAVILION 1-2	TRACK TWO GRAND BALLROOM F-G-H	TRACK THREE GRAND BALLROOM E
10:00 - 10:50	Hardware Hacking Joe Grand	Fighting Organized Cyber Crime Thomas X. Grasso	The Making of atlas atlas
11:00 - 11:50	Googling: I'm Feeling (un)Lucky Greg Conti	The Jericho Forum & Challenge Paul Simmonds, Pamela Fusco, David Mortman, Henry Teng	Remote Pair Programming and Test-driven Development Using Open Source Matt Hargett & Luis Miras
12:00 - 12:50	New Wireless Fun From the Church Of WiFi Renderman, Thorn & H1kari	Beyond Social Engineering Richard Thieme	Internet Wars 2006 Panel
13:00 - 13:50	WarRocketing: Network Stumbling 50 sq. miles in < 60 sec. Rick Hill	Trusted Computing Bruce Potter	
14:00 - 14:50	Hacking Malware Valsmith & Danny Quist	Advanced Attacks Against PocketPC Phones Collin Mulliner	The National Collegiate Cyber Defense Competition Greg White & Kevin Archer
15:00 - 15:50	Rebuilding HARD DRIVES for Data Recovery Scott Moulton	Old Skewl Hacking: Magstripe Madness Major Malfunction	Exploring the Changing Nature of DEFCON over the Past 14 Years Thomas Holt
16:00 - 16:50	Death By 1000 Cuts Johnny Long	Hacking FedEx Kinko's Strom Carlson	Legal Aspects of Internet & Computer Network Defense Robert Clark
17:00 - 17:50	Cyber-crime Foiled Once Again? Amber Schroader & Tyler Cohen	Ask EFF: The Year in Digital Civil Liberties Panel	US-VISIT Chris Paget
18:00 - 18:20	A New Bioinformatics-Inspired and Binary Analysis Scott Miller	Phishing, it starts with "Ph" for a reason. Teli Brown	"What has the NSA done for me lately?" Timothy M O'Neill
18:30 - 18:50			10 Ways To Not Get Caught Hacking On Your Mac Charles Edge aka Krypted
19:00 - 19:50	A Hacker's Guide to RFID Spoofing and Jamming Melanie Rieback	Meet the Fed Panel	Discovering Mac OS X Weaknesses and Fixing Them with the New Bastille OS X Port Jay Beale
20:00 - 20:50	First We Break Your Tag, Then We Break Your Systems Attacks to Rfid Systems Lukas Grunwald	Advanced File System Hiding and Detection Irby Thompson & Mathew Monroe	Mac OS X Security Tools Charles Edge aka Krypted
21:00 - 22:50	Night at the Movies	TCP/IP Drinking Game	Hacker Jeopardy

A NIGHT AT THE MOVIES

HOSTED BY THE DARK TANGENT ON FRIDAY • AUGUST 4 @ 21:00



"'Negadon' is the first film of its kind," said Peter Tatara '05, assistant marketing manager for Central Park Media, the company distributing "Negadon" in North America. "It's a completely computer generated Japanese monster movie. It's like a Godzilla film made entirely with computers."

A staggeringly realistic, film noir style CG film similar to recent blockbuster hits such as Sky Captain & The World of Tomorrow.

Negadon pays homage to a wide variety of 1950's and 60's Japanese monster movies such as Godzilla, Mothra, and other classics which first brought global attention to Japan's then-emerging post-war feature film industry.

The world's first completely computer generated monster movie!

[text from NegadonAttacks.com]

SYNOPSIS:

In the year 2025, the world population explodes to over 10 billion. In search for a new place to live, mankind initiates a space exploration program entitled the Mars Terraforming Project. Step by step, mankind successfully transforms Mars into a habitable planet. But when a Japanese spaceship returning from Mars crashes on the streets of Tokyo, it unleashes a giant and vicious monster. Only Dr. Narasaki and his long-abandoned robot Miroku can save Earth and mankind.

www.negadonattacks.com

DAY 2 SATURDAY AUGUST 5

	TRACK ONE ROYALE PAVILION 1-2	TRACK TWO GRAND BALLROOM F-G-H	TRACK THREE GRAND BALLROOM E
10:00 - 10:50	SOCIAL MESSAGE RELAY Strom Carlson, skrooyoo, datagram & Vidiot	Visual Log Analysis—The Beauty of Graphs Raffael Marty	Ipv6 World Update Kenneth Geers & Alexander Eisen
11:00 - 11:20	802.1x Networking tommEE pickles	Oracle Rootkits 2.0 Alexander Kornbrust	MatriXay: Yuan Fan & Xiao Rong
11:30 - 11:50			Zulu A Command Line Wireless Frame Generator Damon McCoy & Anmol Sheth
12:00 - 12:50	Black Ops 2006 Dan kaminsky	The Evolving Art of Fuzzing Jared DeMott	SAMAEL and NARC dr.kaos, arcon, atlas, beth, digunix
13:00 - 13:50	Hacking UNIX with FreeBSD Jail(8), Secure Virtual Servers Isaac Levy (.ike)	Bridging the Gap Between Static and Dynamic Reversing Luis Miras	IBM Networking Attacks Martyn Ruks
14:00 - 14:50	Service Cloaking and Anonymous Access Michael Rash	Hunting for Metamorphic Engines Mark Stamp & Wing H. Wong	Securing MANET Riley "Caezar" Eller
15:00 - 15:50	Fun with 802.11 Device Drivers Johnny Cache	RE 2006: New Challenges Need Changing Tools Halvar Flake	The Plausible Deniability Toolkit weasel & simple nomad
16:00 - 16:50	UNCLASSIFIED Information Sharing with Non-Traditional Partners Linton Wells	OllyBone: Semi-Automatic Unpacking on IA-32 Joe Stewart	Kiosk Security Peleus Uhley
17:00 - 17:50	Covert Channels using IPv6/ICMPv6 R.P. Murphy	Things That Go "Bump" in the night Marc Weber Tobias & Matt Fiddler	DNS Amplification Attacks Randal Vaughn & Gadi Evron
18:00 - 18:50	Analysing Complex Systems: The BlackBerry Case FX	Safecracking Without a Trace Eric Schmiedl	DNS Abuse Infrastructure and Games Gadi Evron
19:00 - 19:50	Owning the Linksys wrtp54g VOIP Router Arias Hung	Secrets of the Hollywood Hacker! Johnny Long	Blackjacking—Owning the Enterprise via the Blackberry x30n
20:00 - 20:50	Legal Aspects of Computer Self-Defense and Aggressive Self-Defense Robert W. Clark	Automatic Exploit Detection in Binaries Matt Hargett & Luis Miras	
21:00			Hacker Jeopardy

DEFCON MOVIE CHANNEL

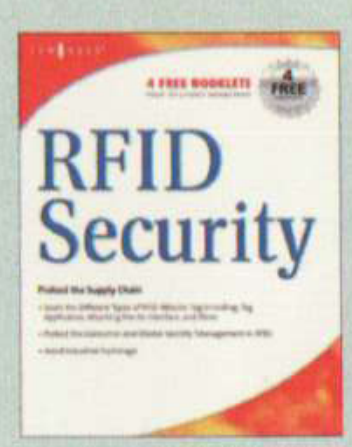
Time	Thursday	Friday	Saturday	Sunday
00:00	dark	Wargames	Hackers	Sneakers
03:00	dark	Real Genius	Antitrust	The Saint
06:00	dark	Brazil	Trainspotting	Harold and Kumar
09:00	dark	Blade Runner	Lawnmower Man	Johny Mnemonic
12:00	dark	Equilibrium	Aeon Flux	Primer
15:00	Tron	Minority Report	Dark City	The Recruit
18:00	Matrix Trilogy	The Hitchhiker's Guide	The 5th Element	Bourne Identity
21:00	Matrix Trilogy	Final Fantasy - Advent Children	The Wizzard	Bourne Supremacy

ORGANIZED BY DC801... 4 YEARS AND COUNTING

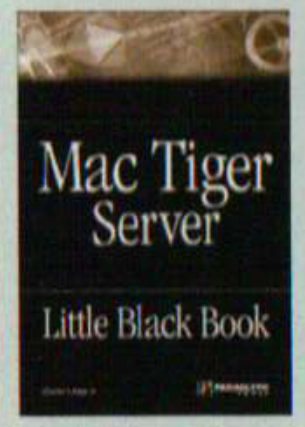
DAY 3
SUNDAY
AUGUST 6

	TRACK ONE ROYALE PAVILION 1-2	TRACK TWO GRAND BALLROOM F-G-H	TRACK THREE GRAND BALLROOM E
10:00 - 10:50	Trust, But Verify Robert J. Hansen	Abuse and the Global Infection Rate Rick Wesson	Corporate Network Spying Andrew Whitaker
11:00 - 11:50	Traffic Analysis Panel Jon Callas	Meme Hacking—Subverting The Ideosphere Broward Horne	A Tale of Two Proxies SensePost
12:00 - 12:50	Graphical Representations of Security Relationships: Awesome or Bullshit? Foofus	EFF v. AT&T: Your World, Delivered (to the NSA) Panel	Advanced Windows Based Firewall Subversion Linoxx
13:00 - 13:50	Phishing Tips and Techniques: Tackle, Rigging, and How & When to Phish Peter Gutmann	How to Create an Anonymous Identity Johan Hybinette	Your Name, Your Shoe Size, Your Identity? What Do We Trust in this Web? Seth Hardy
14:00 - 14:50	Ripples in the Gene Pool Chris Eagle	FEAR!(?) The Census Bureau Steve Dunker	Exploit Writing Using Injectable Virtual Machines Wes Brown & Scott Dunlop
15:00 - 15:50	Malware Repository Requirements Paul Vixie & David Dagon	How the FBI uses NLP on YOU! Brad Smith	
16:00 - 16:50	Awards Ceremonies Hosted by the Dark Tangent		

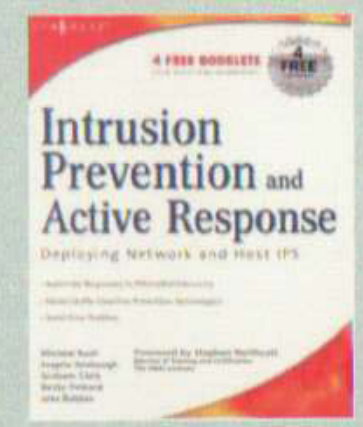
BOOKSIGNINGS



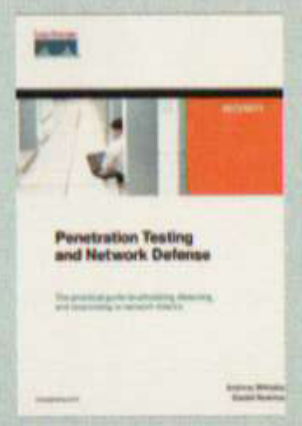
Thorn & Renderman
Fri, 13:00



Charles Edge
Fri, 17:00



Michael Rash
Sat, 19:00



Andrew Whitaker
Sun, 12:00

All booksignings will take place at the
BreakPoint Books Booth located in the vendor area.

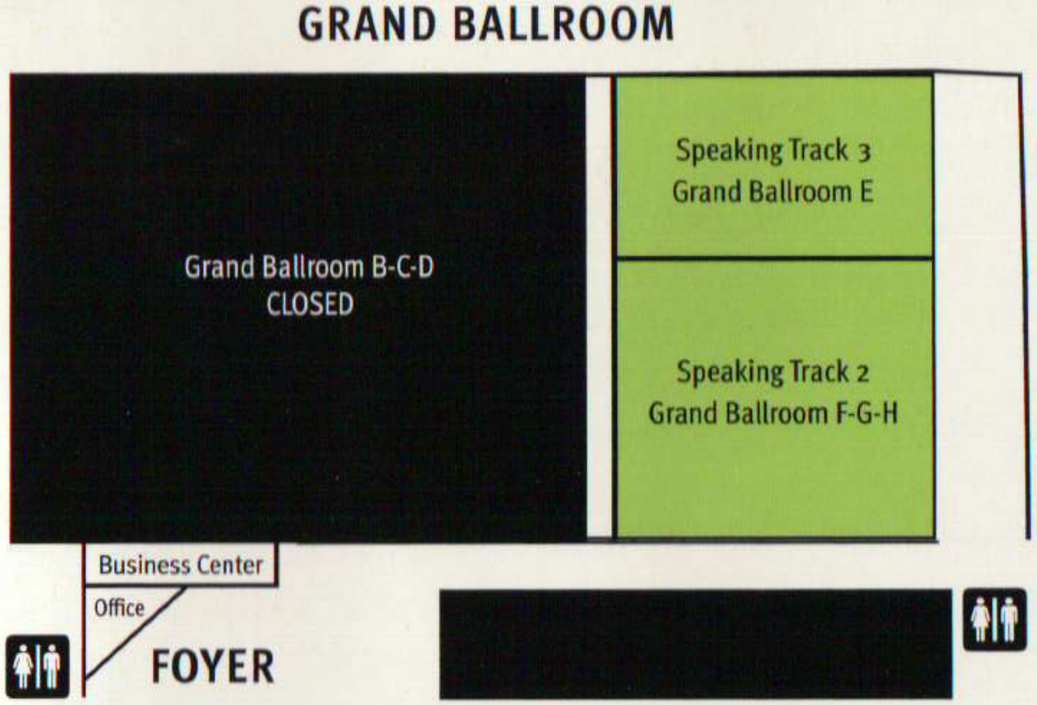


DC GROUPS MEET
Saturday, August 5
20:00 - 23:00
Skybox 206

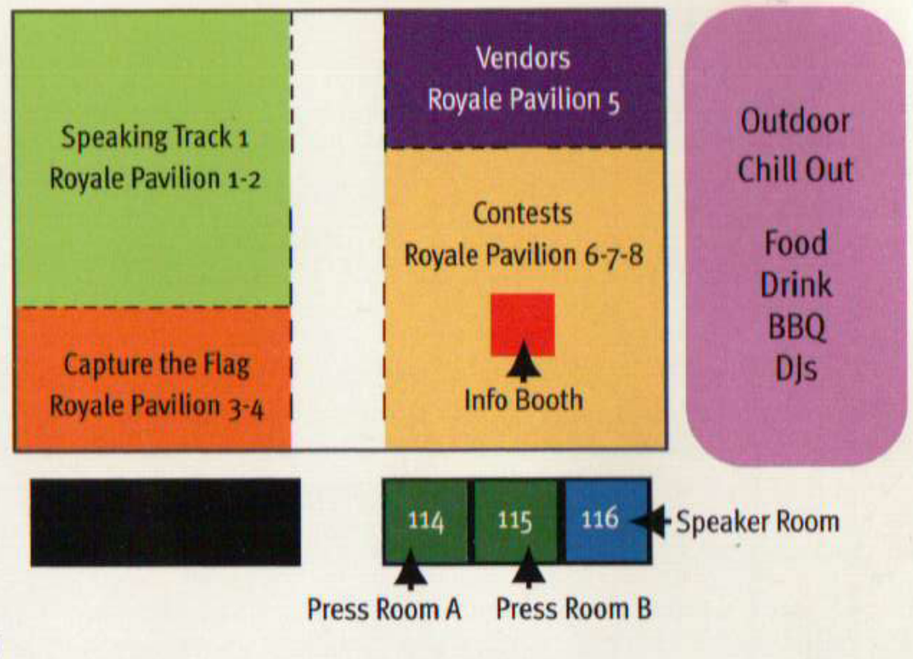
SKYBOXES

	205	206	207	208	209	210	211 & 212
Friday AM	Kenshoto	Lockpick	Metasploit				Public Hang Out
Friday PM	Kenshoto	Forum Meet	Metasploit	Shadowvex	HackerPimps	Irvine UG	Public Hang Out
Saturday AM	Kenshoto	Lockpick	Metasploit	Ninja Networks			Public Hang Out
Saturday PM	Kenshoto	DCG Meet	Avarice	Ninja Networks	Phenoelit	303	Public Hang Out
Sunday AM	Kenshoto	Lockpick	Metasploit				Public Hang Out

ORGANIZED BY GRIFTER







GETTING AROUND

Speaking Track 1: Royale Pavilion 1-2

Speaking Track 2: Grand Ballroom F-G-H

Speaking Track 3: Grand Ballroom E

Black & White Ball: Top of the Riviera Ballroom in the Monaco Tower on the 24th Floor

Contest Area: Royale Pavilion 6-7-8

Dunk Tank: Outdoor area, access through the Vendor and Contest Areas

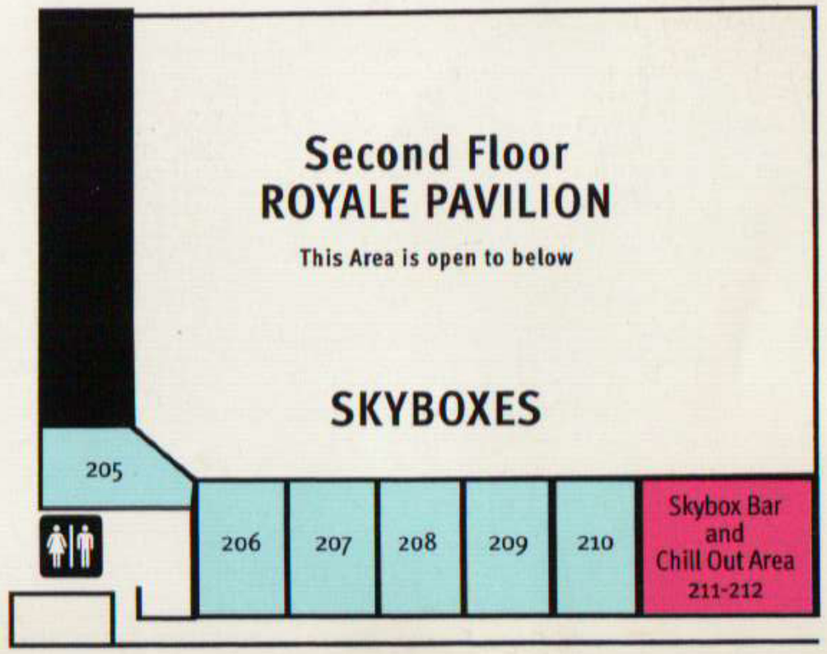
Info Booth: Inside Contest area

Vendors: Grand Ballroom F-G-H

Hacker Jeopardy: Grand Ballroom E

TCP/IP Drinking Game: Grand Ballroom F-G-H





DEFCON

I would like to thank the following people and groups for making this year's DEF CON possible! While there is a metric ass ton of people, if I have not included you it is most likely because I forgot, lost the notes, or you have helped out in years past but not this year. Could be that you decided to help out at the last minute after this went to print as well! As you can see many people make the con possible, as volunteers and because they want to. I raise my beer to you!

First off, without the relentless work of Black Beetle you would not be reading this, or looking at our web site for that matter. She produced the signs, built the web sites, made the conference proceedings and placed the orders for all the cool schwag you see for sale. Designer / Production, super mega organized Ninja.
Special thanks to Neil K who created most of the ninja artwork for the con.

What would DEF CON be with out the Goons? Noid and the whole security crew, Justabill, Riverside, Queeg, The Cap'n, FoxCapt, Carric, Priest, CHS, Danozano, Flea, Kampf, Cyber, Spahkle, Pescador, Teklord, Luna, Decode, Quiet, Arclight, Koz, JD, Kevin E, GM1, CJ, Kruger, Che, Pappy, Freshman, CyMike, Montell, Chosen1, Rik, Nobody, Skydog, Xinc.

The network keeps us humming on-line, and Lockheed has been its master for many many years. He and I would like to thank the whole networking team:
Videoman (7 yrs), Heather (5 yrs), Sqweak (2yrs), effffn (2yrs), Derek/James/Mike(Rant Radio) (3 yrs), and Major Malfunction (179 yrs).

As the space grew, the vendors grew, and that means someone to wrangle them all. That man is known as Roamer, and his team of Ninjas: AlxRogan, Phorkus Maximus, Wiseacre and Evil. A special thanks to Luiz and Aruba for helping get us the great wireless gear at a great price! Thanks to Rescue and Dedhed for managing and staffing the DC Schwag Booth

Hotel: A special thanks to the Riviera for working with us from last year. Alan (congrats on his promotion), Toni (Who got all you guys sleeping rooms), Theresa 'The Queen of the Riviera' for making sure we were all well fed, hydrated, and connected and hotel security for putting up with our antics. You guys roxor.

Wrangling speakers is like herding cats. Chief cat herder is AgentX with his right hand man Paul Proctor and NFF, Code24, Amish, KK, Joe, Rich, AMFYOYO, and all who helped get speakers on stage and off. Thanks to their team we were all able to enjoy the presentations this year!

The contests have really grown, and I want to thank RussR for really reinvigorating this part of DEF CON (as well as his last minute save with helpers for the Schwag booth). Amateur CtF: virus and the DC949/OC crew; Dunk Tank: ericH and Mel; Coffee Wars: Shrdlu and Foofus; War Drive: Thorn; Sub Challenge and Net App: Lost; BeverageCoolingContest: Deviant Ollam; Scavenger Hunt: Siviak and crew; IP Enabled Device: Uber Schnitzle; Janus Wireless Challenge: coderman; Defcon Bots: Kallahar; Lockpick Contest and Village: Doc, Deviant Ollam and Renderman; Slogan Contest: Roamer; Contests Video: melloman; DC Groups Meeting: converge; Extra Sp3c1al thanks to Pyro and danS. Roamer gives shout out to the 303. Winn Schwartau and Nick Farr for Hacker Jeopardy, along with the DC801 crew + Grifter and DedHed for helping with some of the questions.

The Black & White Ball by bink, who books the bands and deals with all the A/V and lighting voodoo. I want to thank all the bands and DJs as well for helping hype up the convention and brining some artistic talent to our line up!

Sponsors: Hey, wait, this is DEF CON! There are no sponsors.

What you see at the con is only a part of what happens the rest of the year. The following people also help out year round, behind the scenes.
Nikita for working with all the submissions, Black Beetle, eta, Dfi, Jeff McNamara for the legal defense skillz, Charel, TheCotMan and the moderators and administrators of the forum: nulltone for watching over it for all those years, and to TheCotMan for stepping up to take it over.

Thank you all! See you guys next year.

— The Dark Tangent —